2017

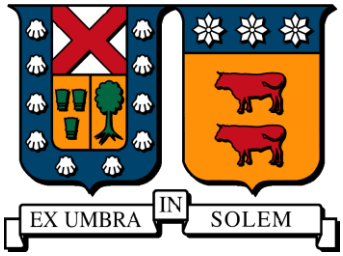
SISTEMA COMPLEMENTARIO PARA MEJORAR LA PERCEPCIÓN DE SEGURIDAD EN PROYECTOS HABITACIONALES DE GRAN ENVERGADURA

GALLARDO STANLEY, MACARENA VICTORIA NATALIA

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA

DEPARTAMENTO DE ELECTRÓNICA

VALPARAÍSO – CHILE



SISTEMA COMPLEMENTARIO PARA MEJORAR LA PERCEPCIÓN DE SEGURIDAD EN PROYECTOS HABITACIONALES DE GRAN ENVERGADURA.

MACARENA VICTORIA NATALIA GALLARDO STANLEY

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL TELEMÁTICO

PROFESOR GUÍA: MARCOS ZUÑIGA

PROFESOR CORREFERENTE: DANIEL ERRAZ

MARZO- 2017

Agradecimientos

Agradecimientos generales al Profesor Marcos Zuñiga y Daniel Erraz por tener siempre la disponibilidad y disposición de guiar, corregir y ayudarme; a la Inmobiliaria Fundamenta por presentar un desafío tan interesante y confiar en la capacidad del equipo para desarrollarlo, a Francisco Martinez, contraparte de la Inmobliaria Fundamenta, por tener la disposición de ayudar y brindar información acerca de los proyectos y el modo de funcionamiento de la empresa, a las Secretaría tanto del Departamento de Electrónica como de Telemática por aclarar cualquier duda con respecto al protocolo correspondiente a la memoria, a los profesores de los módulos del plan de Memorias Multisciplinarias por ser un aporte en cada etapa de este desafío y a todos los profesores que fueron parte de mi carrera universitaria.

Agradecimientos a mis amigos Franco, Ricardo y Gabriela por el apoyo durante todos estos años, a mi pareja Marcelo por distraerme en los momentos más importantes.

Dedicatoria

Dedicado a mis padres y mi hermano por su apoyo incondicional en todos los momentos de mi vida, por las energías brindadas en este último periodo y el amor entregado.

Sistema Complementario para mejorar la percepción de seguridad en proyectos habitacionales de gran envergadura

Macarena Victoria Natalia Gallardo Stanley

Memoria para optar al título de Ingeniero Civil Telemático

Profesor Guía: Marcos Zuñiga

Abril – 2017

Resumen

Este proyecto está orientado al desarrollo de un sistema complementario a los actuales métodos de seguridad implementados en los proyectos habitacionales de gran envergadura, automatizando el control de acceso al inmueble.

El proyecto se ha desarrollado en base a un nodo central mediante la plataforma Raspberry Pi 3 Modelo B, el cual es el encargado de obtener y procesar información mediante la tecnología inalámbrica Bluetooth desde el usuario al sistema.

Además, mediante una aplicación móvil ejecutada sobre smartphones y tablets con sistema operativo Android, se solicite el acceso al inmueble y se genere la petición del ascensor.

También tiene por objetivos interesar a futuros clientes sobre la tecnología IoT (Internet of Things, en español, Internet de las Cosas) a un bajo costo de implementación, como casas comerciales, universidades, organismos del Estado, bibliotecas y usuarios comunes, con el fin de resguardar y controlar el acceso a la propiedad.

Para el desarrollo de este proyecto se implementa un sistema de arquitectura Cliente-Servidor. El módulo cliente es la aplicación usuaria en el equipo Android desde la cual se generan las peticiones y se recibe su estado; y el servidor alojado en la Raspberry, es el encargado de ingresar a los usuarios con su nivel de acceso, procesar las peticiones y emitir una respuesta.

El desarrollo de este proyecto se lleva a cabo a través del programa de Memorias Multidisciplinarias, de la Universidad Técnica Federico Santa María.

Palabras claves: Android, aplicaciones móviles, seguridad, Bluetooth, control de acceso.

Complementary system for improving the perception security in housing projects.

Macarena Victoria Natalia Gallardo Stanley

Final Project Report towards the fulfillment of Ingeniero Civil Telemático, Mayor in Telecommunications degree (6 year engineering program)

Advisor: Marcos Zuñiga

Abril – 2017

Abstract

This Project is oriented to the development of a complementary system to current security methods implemented in the housing projects of great magnitude, by automating control of access to the property.

The project has been developed based on a central node using the Raspberry Pi 3 model B platform, which is responsible for obtaining and processing information using Bluetooth wireless technology from the user to the system.

In addition, through a mobile application running on smartphones and tablets with Android operating system, access request to the property and request of the lift is generated.

Also, it aims to interest future customers about IoT technology (Internet of Things) to a low cost of implementation, such as trading houses, universities, agencies of the State, libraries and common users, in order to protect and control access to the property.

A system of client-server architecture is implemented for the development of this project. The client module is the user application on the computer Android from which requests are generated and received its status. and the server hosted in the Raspberry, is responsible for entering users with their level of access, process the request and issue a response.

This project is carried out through the Multidisciplinary Thesis Program, of the Universidad Técnica Federico Santa María.

Keywords: Android, mobile app, security, Bluetooth, Access control.

Glosario

IoT	Internet of Things
RFID	Radio Frecuency Identification
NFC	Near Field Communication
SSL	Secure Sockets Layer
HICO	High Coercivity
LOCO	Low Coercivity
PCA	Principal Component Analysis
LDA	Linear Discriminant Analysis
EBGM	Elastic Bunch Graph Matching
QR	Quick Response
SMS	Short Message Service
JIT	Just In Time
GPS	Global Positioning System
API	Application Programming Interface
BLE	Bluetooth Low Energy
ART	Android Runtime
ISM	Industrial, Scientific and Medical
MAC	Media Access Control
CPU	Central Processing Unit
USB	Universal Serial Bus
RAM	Random Access Control
SD	Secure Digital
GPIO	General Purpose Input/Output
SMTP	Simple Mail Transfer Protocol
JDK	Java Devolpment Kit
SDP	Session Description Protocol
UUID	Universally Unique Identifier
OBEX	Object Exchange
TCP	Transmission Control Protocol

Tabla de contenido

Índice de ilustraciones

Índice de Tablas

1. Capítulo: Introducción y objetivos

A través del programa de Memorias Multidisciplinarias, se analiza e implementa el desafío propuesto por la inmobiliaria Fundamenta "*¿Cómo mejorar la percepción de seguridad de proyectos habitacionales de gran envergadura de manera no invasiva?*

Para el desarrollo de este desafío se conforma un equipo junto a Henrich Reinking, estudiante de ingeniería civil electrónica.

1.1. Introducción

"La seguridad es la ausencia de peligro y riesgo".

La seguridad es uno de los temas más debatidos y tratados por las autoridades, la clase política y la población en general. La seguridad es uno de los aspectos prioritarios para la sociedad, ya que la ausencia de ésta produce una baja calidad de vida.

El problema raíz es el aumento considerable de la inseguridad social, donde las personas se sienten cada día más vulnerables, más desprotegidas, sintiendo que la violencia cada día aumenta más.

Es por lo anterior, que la gran mayoría de las personas busca viviendas que le brinden el grado de seguridad necesario para un buen vivir, con sistemas de seguridad robustos y simples de usar.

Los departamentos durante muchos años fueron considerados las viviendas que alcanzaban los niveles más altos de confiabilidad en términos de seguridad. Hoy, por el contrario, esta cifra, cada vez va disminuyendo más, debido a lo fácil que es vulnerar los sistemas de seguridad que implementan. Una gran parte de los robos que los afectan se producen por usuarios del mismo edificio como arrendatarios, propietarios, visitas, trabajadores, entre otros, debido a que no existe un control ni registro que perdure con el tiempo.

La gran mayoría de los sistemas de seguridad utilizados por proyectos habitacionales de gran envergadura, quedan obsoletos al poco tiempo de implementación, debido a la complejidad de éste, al tiempo que tarda en ser utilizado, la poca cercanía con el usuario y a la carga de solicitudes que pueda tener el conserje que sobrepase los protocolos establecidos.

Por lo expuesto anteriormente, el propósito de esta memoria es desarrollar un sistema que brinde una sensación de seguridad para sus usuarios de una manera no invasiva, que destaque por su simpleza y confiabilidad.

El sistema por desarrollar debe cumplir con ciertas exigencias como “no invasivo”, término que va enfocado a la retención de la visita o residente por periodos prolongados de tiempo; de fácil uso, orientado a los usuarios, ya sean propietarios, arrendatarios, visitas y todo trabajador del inmueble; que sea capaz de controlar flujos de personas, ya que se consideran proyectos habitacionales de gran envergadura y difíciles de vulnerar.

Durante el desarrollo de esta memoria, se analizarán las diferentes aristas de este sistema, enfocándose en el trabajo del área telemática. Se definirán las tecnologías a utilizar, el progreso del sistema con sus algoritmos, se probará la factibilidad de éste y se precisarán las conclusiones.

1.2. Alcance

El alcance del proyecto a desarrollar e implementar durante esta memoria se enfoca en la definición de tecnologías como medio de comunicación de los distintos módulos del sistema, desde la aplicación móvil hasta el servidor.

En la definición de tecnologías como medio de comunicación, se analizarán las diferentes tecnologías existentes que cumplan con los requisitos del sistema y se definirán aquellas que presenten una mayor cercanía a los ejes de control de flujo y sean simples de interactuar.

En el área de aplicación móvil, se desarrollará una aplicación que permita al usuario interactuar con el sistema de manera simple y segura, la cual contendrá las opciones disponibles de acuerdo con el nivel de acceso que tenga registrado el usuario.

Dentro de la aplicación del servidor, se desarrollará un programa que sea capaz de interpretar los mensajes enviados por la aplicación y dar respuestas de aquellas solicitudes.

El proyecto se realiza a nivel de prototipo, por lo que se espera obtener resultados que permitan demostrar y abordar una solución de acuerdo con los intereses de la contraparte, que cumplan con sus expectativas de seguridad y tecnología.

1.3. Definición del problema

El problema principal es el aumento incontenible de inseguridad social que existe hoy en día, donde las personas no se sienten seguras ni en su propio hogar y debido a esto han buscado nuevas formas de protección.

De acuerdo a un estudio desarrollado por Paz Ciudadana y Cfk Adimark llamado “Delincuencia y Opinión Pública” realizado a 52 comunas -36 comunas del gran

Santiago- y a personas mayores de 18 años que residen en hogares, se obtiene los siguientes índices en materia de seguridad [1].

- En comparación con un año atrás, piensa usted que la cantidad de delincuencia en su comuna: ¿mayor, igual o menor?

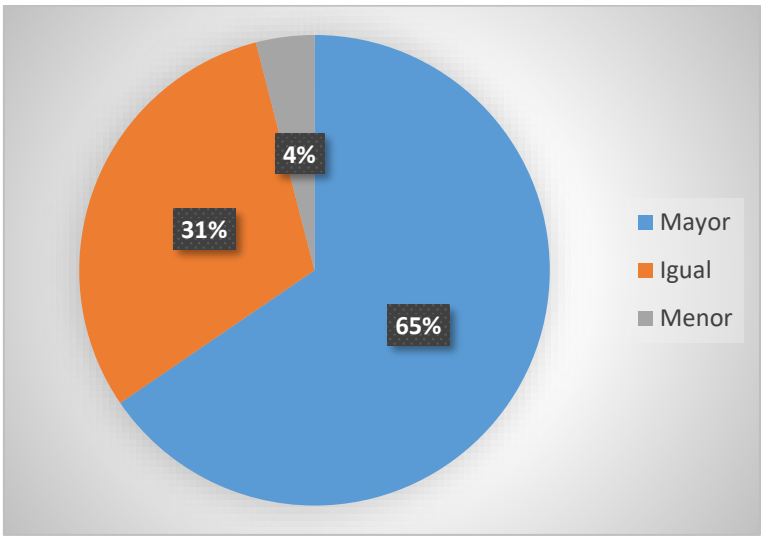


Ilustración 1.1.1: Gráfico cantidad de delincuencia.

Fuente: Delincuencia y Opinión Pública.

- ¿Usted diría que la delincuencia en su comuna es hoy más violenta, menos violenta o igual de violenta?

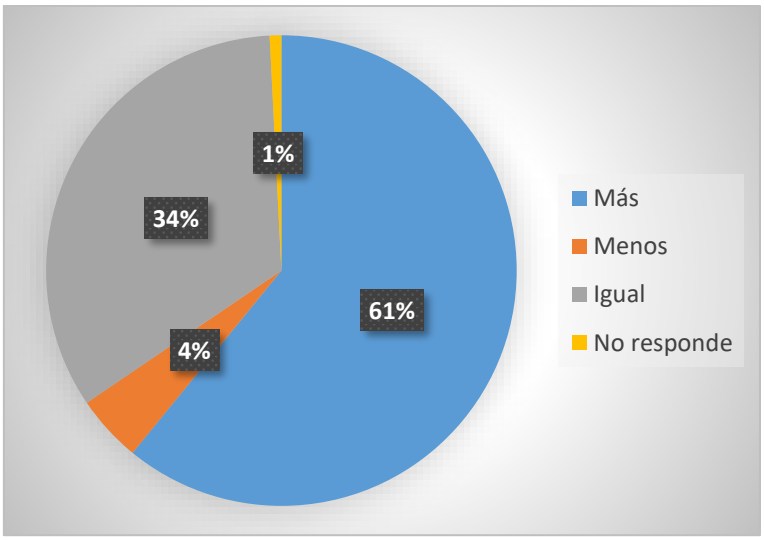


Ilustración 1.1.2: Gráfico nivel de violencia.

Fuente: Delincuencia y Opinión Pública.

- ¿Usted cree que en el futuro, la delincuencia en su comuna aumentará, disminuirá o se mantendré igual?

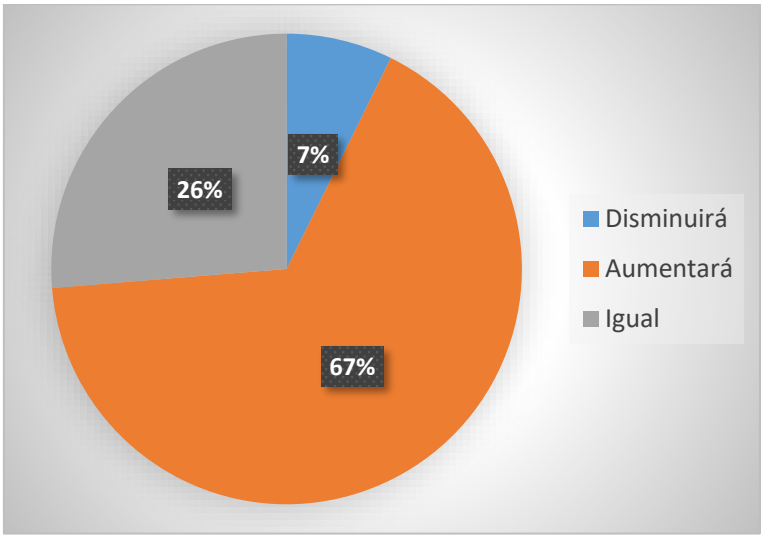


Ilustración 1.1.3: Gráfico de incremento de delincuencia.

Fuente: Delincuencia y Opinión Pública.

- Frecuencia con que siente temor de ser asaltado o robado dentro de su hogar en las noches.

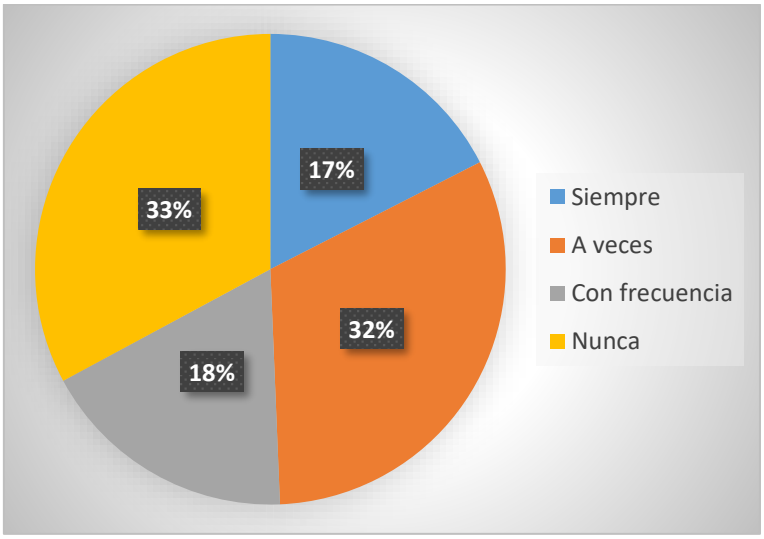


Ilustración 1.1.4: Gráfico frecuencia de temor.

Fuente: Delincuencia y Opinión Pública.

De los gráficos anteriores es posible apreciar el aumento de la percepción de inseguridad, donde las personas se sienten cada día más vulnerables, desprotegidas, sintiendo que la violencia cada día aumenta más. El 65% siente que la delincuencia aumentó en comparación con el año anterior y más del 65% ha sentido temor de ser asaltado o robado en su hogar por las noches.

Las siguientes imágenes representan una encuesta de satisfacción realizada por la inmobiliaria Fundamenta en las comunas de Providencia, Santiago y La Dehesa [2].

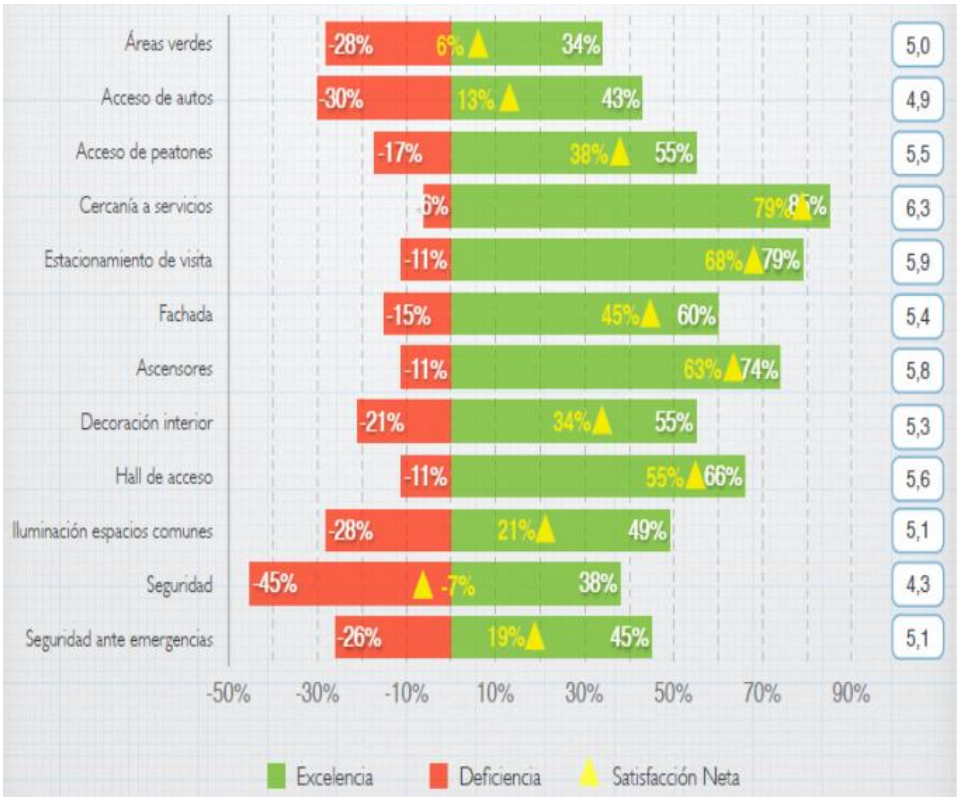


Ilustración 1.1.5: Encuesta de satisfacción Providencia.

Fuente: Inmobiliaria Fundamenta.

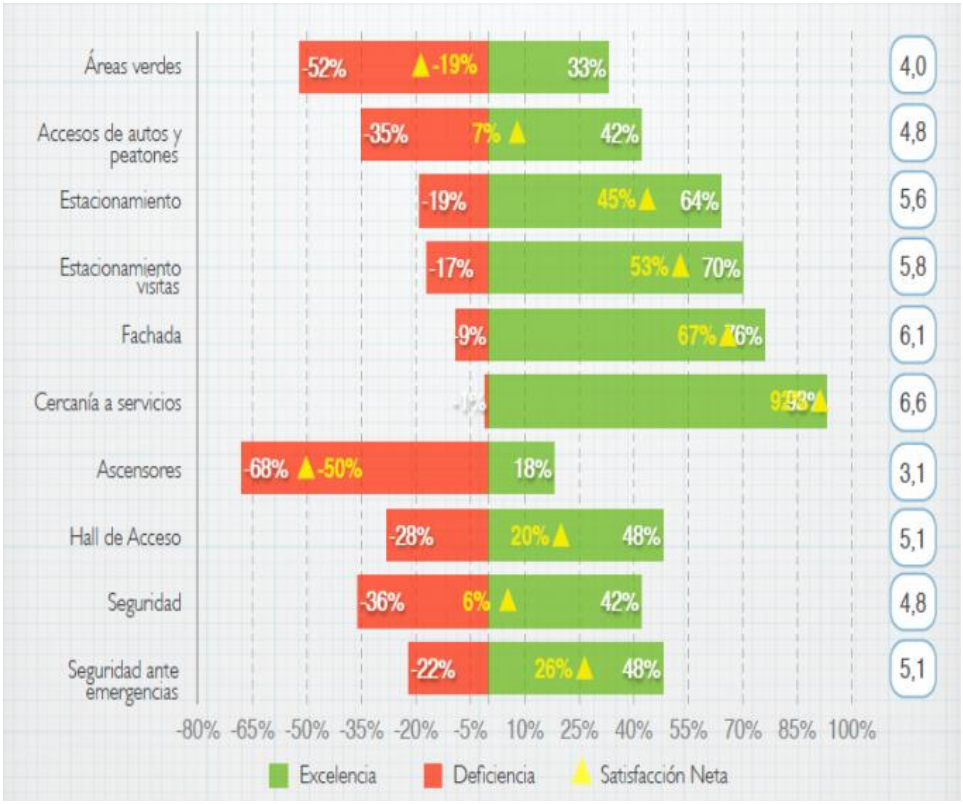


Ilustración 1.1.6: Encuesta de satisfacción Santiago.

Fuente: Inmobiliaria Fundamenta.

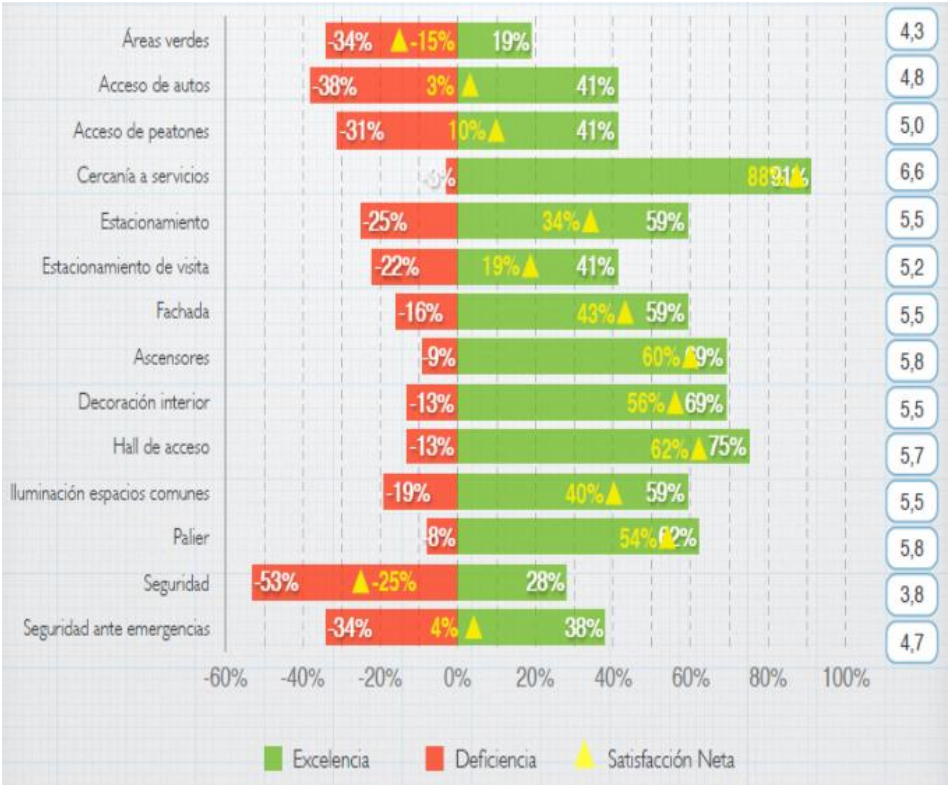


Ilustración 1.1.7: Encuesta de satisfacción.

Fuente: Inmobiliaria Fundamenta.

De acuerdo a las imágenes anteriores, se puede apreciar que las evaluaciones más bajas corresponden a seguridad, independiente del sector en el que se encuentra ubicado el inmueble.

Según lo anteriormente descrito, se observa que la inseguridad social es un problema incontenible que afecta a diversos sectores del país, independiente del sector escogido para vivir.

1.4. Objetivos

A continuación, se definen los objetivos generales y específicos desarrollados en este proyecto.

1.4.1. Objetivos Generales

- Creación de un sistema de seguridad no invasivo y eficiente para proyectos habitacionales de gran envergadura.
- Aumentar la percepción de seguridad en los habitantes de edificios de gran envergadura.

1.4.2. Objetivos Específicos

- Configuración de un servidor local, que contenga la base de datos y el software necesario para la comunicación entre distintos dispositivos.
- Creación de una aplicación móvil usuaria, la cual sea capaz de emitir solicitudes vía Bluetooth.
- Utilizar como mecanismo de acceso al inmueble un celular inteligente.
- Utilizar la tecnología inalámbrica Bluetooth.

1.5. Organización del documento

En la presente sección se describe brevemente el contenido de cada capítulo.

CAPITULO I: Introducción y Objetivos

Se introduce el tema de memoria y se describen los objetivos generales y específicos.

CAPITULO II: Estado del Arte

Se comenta y explica el funcionamiento de los sistemas de seguridad más utilizados alrededor del mundo, los cuales podrían satisfacer las necesidades a plantear.

CAPITULO III: Análisis del estado del arte y comparación entre sistemas de seguridad implementados.

Se analizan los sistemas de seguridad implementados hoy en día y se realiza una comparación entre las distintas tecnologías utilizadas.

CAPITULO IV: Identificación de elementos claves y selección de tecnologías.

Se identifican los principales elementos que se deben tener en consideración para pensar en una propuesta de solución. A partir de lo anterior, se escogen las tecnologías más acordes al problema.

CAPITULO V: Requisitos del sistema

Se plantean los requisitos funcionales y no funcionales mínimos que cumplan con lo solicitado por el cliente.

CAPITULO VI: Diseño y desarrollo de la solución

En este capítulo se muestra al lector los distintos diagramas para el entendimiento del problema y se comienza a desarrollar la solución

CAPITULO VII: Programación

Se plantea la solución y la programación que existe tras esta. Se presentan las bibliotecas y módulos utilizados.

CAPITULO VIII: Aplicación y pruebas

Se presenta el desarrollo de la aplicación y las pruebas realizadas para validar y verificar el correcto funcionamiento de la solución.

CAPITULO IX: Conclusiones y resultados

En este ítem se informan las conclusiones más significativas luego del desarrollo, los pasos a seguir y los resultados.

2. Capítulo: Estado del Arte

En este capítulo se analizarán los sistemas de seguridad y control de acceso implementados con mayor reconocimiento a nivel mundial. Además, se mencionará la tecnología Bluetooth en el uso de aplicaciones móviles y se introducirá el sistema operativo Android.

2.1. Sistemas de seguridad y control de acceso reconocidos mundialmente

La seguridad en la vivienda siempre ha sido y será un punto importante a la hora de adquirir nuevos inmuebles, arrendar o visitar. Es por esto, que algunas empresas como las inmobiliarias predisponen una gran cantidad de recursos para hacer lugares más seguros para el usuario.

A lo largo de la historia, se han implementado diversos sistemas y tecnologías para controlar el acceso y brindar percepción de seguridad a proyectos inmobiliarios de gran envergadura, las cuales varían de acuerdo con su precisión, robustez, eficiencia y cuán invasivo sea.

En la actualidad, existen variadas soluciones. Se detallarán las más eficaces y sostenibles durante el tiempo.

2.1.1. Sistema de seguridad basado en teclado numérico

Los sistemas de seguridad basados en códigos numéricos son uno de los más populares y económicos del mercado. Este sistema se conforma por un teclado numérico que se encuentra enlazado con un sistema electrónico y mecánico, el cual es el encargado de gestionar el acceso.

El funcionamiento consiste en que cada usuario maneja su propio código, alrededor de ocho caracteres, el cual es la llave de acceso al inmueble. Cuando el usuario desee ingresar a la vivienda, debe introducir su código en los teclados de acceso al edificio. Si el código es correcto se permite el acceso.

La validación de los códigos se realiza mediante un programa, el cual posee acceso a una base de datos, donde se encuentran todos los usuarios registrados con su código. Por esto, es el programa el encargado de consultar la base de datos y verificar que efectivamente el código, posea el acceso para ingresar. [3]

Algunas versiones de este sistema funcionan, registrando al usuario en la base de datos cada vez que solicita el acceso al inmueble, para así, poder contar con un registro detallado del acceso con fecha y hora.

También, existen versiones en las que todos los usuarios del sistema poseen el mismo código, lo que se traduce en cambios periódicos del dicho código.

Una de las ventajas principales que posee este sistema, es la simplicidad de uso para el usuario, ya que no requiere portar ningún implemento extra, no requiere conocimientos previos y no necesita conocer la tecnología involucrada.

Por otra parte, los estudios señalan que el ser humano en promedio memoriza solo 6 dígitos en menores de 40 años, por lo que no sería aconsejable contar con un código mayor de 6 dígitos. Además, este sistema no posee autentificación de usuario, ya que no existe ningún tipo de procedimiento que permita al sistema saber, si la persona que está ingresando el código, cuenta con los privilegios para acceder.

Ilustración 2.2.1: Teclado numérico para control de acceso.

2.1.2. Sistema de seguridad con tecnología RFID

La tecnología RFID, viene del inglés *Radio Frecuency Identification* o Identificación por Radio Frecuencia.

Los sistemas que implementan la tecnología RFID cuentan con dos tipos de accesorios: *RFID lector* y *RFID tag.*

Los RFID tag, normalmente poseen forma de llaveros cuando son implementados como sistema de acceso, con lo cual, cada usuario posee uno. Estos poseen un identificador único, asociado a cada persona. [4]

Los RFID lector, son los lectores que interactúan los RFID tag y encargados de obtener su identificador. Son ubicados en todos los accesos del inmueble. [5]

El sistema es complementado por un programa que verifica, a través de consultas a la base de datos, que el identificador de RFID tag asociado a un usuario, cuente con el permiso de acceso al edificio.

Existen dos tipos de RFID tag, los pasivos y los activos.

Los RFID pasivos, operan en el rango de frecuencia hasta los 960 [MHz] y no contienen batería propia, por lo cual, funcionan por inducción de energía, emitida desde el lector, lo que se traduce, en la disminución de su distancia de operación, alcanzando como máximo una distancia de 20[cm] entre el lector y el tag.

Los RFID activos, operan en el rango de frecuencia de 433[Mhz] hasta los 5,8[Ghz], poseen una fuente de poder dedicada para emitir una señal con su código de identificación, lo cual, permite un mayor rango de operación, alcanzando los 3,4[m]. [6] [7]

Cabe destacar, que el precio de adquisición y de mantenimiento es mucho más elevado en los RFID tag activos, que, en los pasivos, por el hecho de funcionar con una fuente de poder propia. Por otro lado, los RFID pasivos presentan más probabilidad a perturbaciones debido al rango de frecuencia en el que operan. [8]

En cuanto a la seguridad de esta tecnología, hay estudios que sostienen la factibilidad de hackeo, tanto en los dispositivos lectores como en los tag. Debido a su comunicación inalámbrica y a su cifrado se realizan ataques del tipo Man-In-The-Middle. [9] [10]

Los sistemas de seguridad basados en RFID, están siendo ampliamente utilizados, por su precio y seguridad. En Chile, se tiene el caso de las autopistas de Santiago, las cuales funcionan con esta tecnología al momento de cobrar por su uso, sustituyendo a las plazas de peajes.

Ilustración 2.2: Sistema de control de acceso vehículos vía RFID.

Ilustración 2.3: Sistema completo RFID.

2.1.3. Sistema de seguridad con NFC

El sistema NFC es una tecnología de comunicación inalámbrica de corto alcance y alta frecuencia que permite el intercambio de datos. Funciona en la banda de 13.56 MHz y su tasa de transferencia puede alcanzar los 424 Kbits/s. Se utiliza principalmente para identificar y validar. [11]

Las ventajas son que su uso es transparente a los usuarios, es half dúplex, las transmisiones pueden utilizar encriptaciones de seguridad como SSL y al trabajar a distancias reducidas hace difícil que exista un tercer dispositivo que interfiera la comunicación. [12]

Dentro de las desventajas, se aprecia que es de corto alcance, ya que su tecnología no permite distancias mayores a los 20 cm y actualmente existen diversas aplicaciones que vulneran la seguridad de los dispositivos móviles, encendiendo el NFC y transmitiendo la información a otro teléfono, extrayendo sin consentimiento del usuario todos los datos que son enviados a través de esta. Lo anterior, es conocido como el ataque relay. [13]

La tecnología NFC utiliza dos modos para establecer la comunicación:

- Modo pasivo: el dispositivo iniciador genera un campo electromagnético y el dispositivo de destino, se comunica con este, modulando la señal recibida, por lo que el dispositivo de destino obtiene la energía necesaria para funcionar del campo electromagnético.
- Modo activo: tanto el dispositivo iniciador como el de destino, se comunican generando su propio campo electromagnético, por lo que ambos necesitan una fuente de alimentación para funcionar.

Los celulares inteligentes o Smartphones con NFC, pueden operar con el modo de comunicación de emulación NFC card, el cual, le permite al móvil, actuar como una smartcard.

Para ser implementado como un sistema de seguridad, es necesario contar con una base de datos, la cual debe contener todos los registros de los usuarios con sus permisos correspondientes.

Además, se debe contar con un NFC lector y una tarjeta NFC. Una vez que la tarjeta se acerque al lector, este último obtiene la información, para luego ser procesada y verificada, comparándola con los registros de la base de datos. Si el usuario cuenta con el permiso, se activa la acción de acceso.

Ilustración 2.4: Control de acceso NFC vía smatphone.

Ilustración 2.5: Llaveros NFC.

Ilustración 2.6: Receptor NFC.

2.1.4. Sistema de seguridad basado en Huella Dactilar

Este sistema de seguridad posee la capacidad de controlar el ingreso de los usuarios, a través del reconocimiento de su huella dactilar.

Una huella está formada por una serie de crestas y surcos, localizados en la superficie del dedo. La singularidad de una huella puede ser determinada por el patrón de crestas y surcos, así como el patrón de detalles. [14]

- Patrón basado en detalles:
  Se crea un mapa con la ubicación relativa de detalles sobre la huella. Para aplicar esta técnica las imágenes deben ser de buena calidad.

Ilustración 2.7: Tipos de detalles de huellas.

- Patrón de crestas y surcos:
  Localiza un punto según crestas y surcos, para luego ser clasificado. Separando el número de crestas presentes en cuatro direcciones.

Una vez capturada la imagen de la huella, se realiza el reconocimiento de esta. El sistema compara con las imágenes alojadas en la base de datos. En caso de coincidencia, permite el acceso. [15]

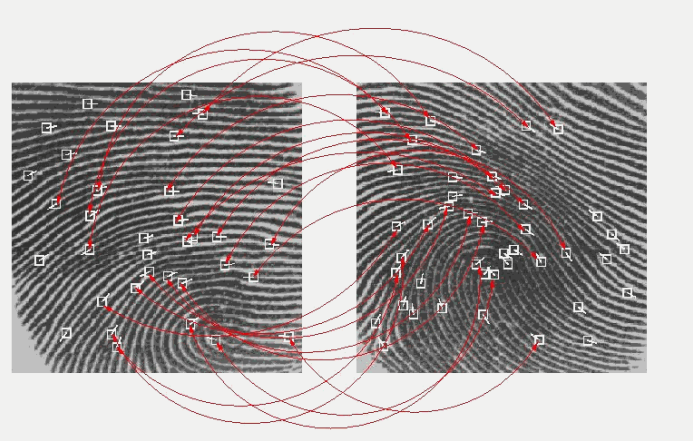


Ilustración 2.8: Comparación huella dactilar.

En lugares que cuentan con varios usuarios y con un flujo de personas considerable, este sistema se complementa con un panel numérico. De esta forma, el usuario ingresa su código y huella, el sistema reconoce al usuario mediante el código ingresado y verifica la imagen asociada con la huella ingresada. En caso de coincidir y que este cumpla con los atributos de ingreso, le permite el acceso. Complementarlo con un código de usuario, permite al sistema hacerlo más robusto y disminuir los tiempos de consultas.

El sistema de seguridad basado en huella dactilar es uno de los más utilizados por grandes tiendas y empresas.

Ilustración 2.9: Dispositivo receptor huella dactilar.

2.1.5. Sistema de seguridad con banda magnética

El sistema de seguridad con banda magnética es uno de los sistemas de control de acceso, más utilizados a nivel mundial. Consta de una tarjeta, la cual contiene toda la información que necesita el sistema para poder autenticar al usuario.

Para la implementación de este sistema es necesario contar con la tarjeta y un lector de banda magnética. Para su funcionamiento, es fundamental que el lector permanezca en contacto durante toda la lectura con la banda magnética de la tarjeta y que esta última, se mantenga en movimiento. No se requiere una velocidad constante, por lo que puede ser proporcionado manualmente.

Existen dos tipos de banda magnética, las Hi-co y las Lo-co.

Las primeras son codificadas con un alto campo magnético, lo que provoca que los datos codificados sean menos propensos a ser borrados de manera accidental cuando son expuestas a un campo magnético externo. Estas son ideales para control de acceso debido al gran uso que se les da. [16]

Las segundas son menos comunes y son buenas para aplicaciones de corto tiempo. Son codificadas en un campo magnético de baja intensidad.

Dentro de las ventajas se encuentra la durabilidad de hasta dos años de la banda magnética. Por el contrario, las desventajas de utilizar este sistema, es la escasa implementación de métodos de criptografía, lo cual, lo vuelve muy vulnerable a la clonación, por lo que este tipo de sistemas se encuentra en retirada.

Al igual que los sistemas anteriores, debe contar de manera complementaria con una base de datos que contenga los registros y permisos de todos los usuarios, además, de un sistema que gestione el control de acceso.

Ilustración 2.10: Lector de banda magnética y tarjeta.

2.1.6. Sistema de seguridad con reconocimiento facial

El sistema de seguridad con reconocimiento facial es implementado principalmente en edificios con un alto grado de seguridad y gran cantidad de personas. Se trabaja con cámaras y un software de detección de rostros. Tiene dos modos de funcionamiento, la identificación y la verificación.

El modo de funcionamiento de identificación compara el rostro capturado, a través de las cámaras, con una serie de imágenes guardadas en una base de datos. Por el contrario, el modo de funcionamiento de verificación compara la imagen o rostro capturado por la cámara, con el de la persona que haya utilizado algún tipo de identificador de identidad para el acceso, a través de un torniquete o puerta electrónica.

El funcionamiento como sistema de seguridad para acceso sigue los siguientes pasos:

- Obtención de la imagen: el sistema a través de cámaras detecta un rostro y captura la imagen.
- Escala de rostro: determina el tamaño del rostro desde la imagen y la escala al tamaño y posición predeterminados para procesar.
- Procesa imagen: una vez obtenida la imagen en tamaño y posición preestablecidas, se localizan los componentes del rostro, se normaliza a través de componentes geométricos como la distancia entre los ojos, comisura de los labios, posición de la nariz o medición de ángulos de la cara, también puede aplicar filtros y/o histogramas sobre la imagen con el fin de mejorarla.
- Extracción de características: entrega información para distinguir entre los rostros de diferentes personas.

- Reconocimiento: compara los vectores obtenidos de la extracción de características con los guardados en la base de datos. Si cumple con el porcentaje de reconocimiento establecido se concede el acceso, y de lo contrario se niega.

Hay dos enfoques predominantes aplicados en sistema de seguridad facial: el geométrico -basado en los rasgos del individuo- y fotométrico – basado en lo visual-. [17]

Algoritmos de reconocimiento facial: [18]

- PCA – Análisis de componentes principales
  Técnica impulsada por Kirby & Sirivich. La imagen a tratar y las fotografías a sondear deben ser del mismo tamaño y deben ser normalizadas previamente. Luego viene una etapa de reducción de información que no es útil y descompone de manera precisa la estructura facial en componentes ortogonales conocidos como Eigenfaces, por lo que cada imagen puede ser presentada como la suma ponderada de estos.
  La utilización de este algoritmo requiere la cara completa de frente.
  La ventaja de esta técnica es la capacidad de reducción de datos necesarios para identificar al individuo.
- LDA – Linear Discriminant Analysis
  Es una aproximación estadística para clasificar muestras de clases desconocidas basadas en enrenamiento de clases conocidas. Esta técnica maximiza la varianza entre clases y minimiza la varianza de cada clara.
- EBGM – Elastic Bunch Graph Matching
  Esta técnica considera que las imágenes faciales reales tienen muchas características no lineales que no son tratadas en los métodos anteriores, como la variación de la iluminación, postura y expresión.
  La forma de proceder es exponer la imagen a un filtro de gabor, el cual es usado para detectar formas y extraer características utilizando el procesamiento de imagen. [19]

El sistema de reconocimiento facial tiene la ventaja de que éste es un método no intrusivo, es decir, los datos pueden ser obtenidos incluso sin que el sujeto se percate de ello. Este sistema tiene las dificultades de reconocimiento cuando la variación entre las imágenes de distintos sujetos es muy pequeña o cuando la variación entre imágenes de una misma persona es muy amplia, esto puede ser provocado e intensificado cuando dichas imágenes hayan sido adquiridas en diferentes condiciones ya sea de iluminación, posición o calidad.

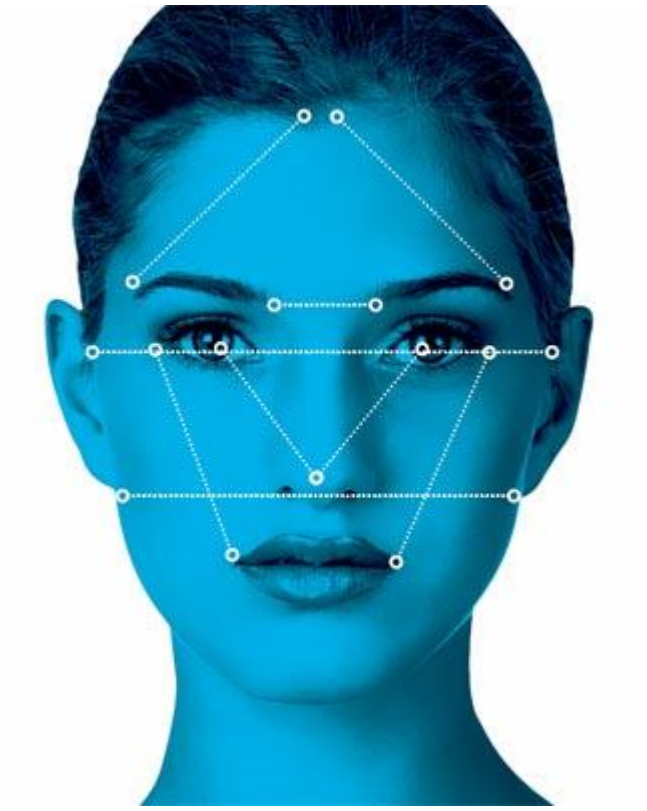


Ilustración 2.11: Puntos de reconocimiento facial.

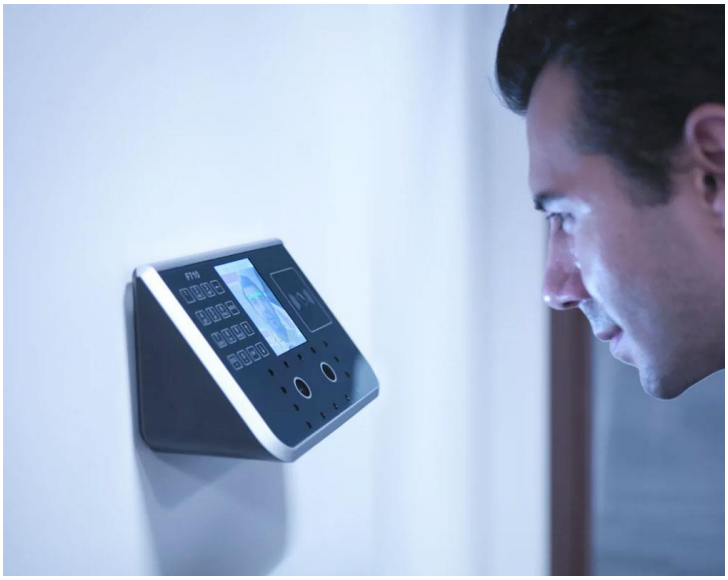


Ilustración 2.12: Sistema de reconocimiento facial.

2.1.7. Sistema de seguridad con circuito cerrado de televisión

Los sistemas de seguridad con circuito cerrado de televisión se encuentran presentes casi en la totalidad de edificios, tanto empresariales como habitacionales.

El sistema se compone de cámaras, por cable o inalámbricas, que transmiten sus capturas de imágenes, para luego ser grabadas, pudiendo acceder a material de días anteriores.

La conexión remota al sistema de seguridad, vía internet, ha hecho un plus para el aumento de percepción de seguridad de los usuarios, dado que ellos pueden acceder mediante una plataforma y revisar las imágenes correspondientes a su hogar.

El rol de los conserjes es fundamental, ya que es su responsabilidad vigilar los que sucede en las pantallas y son estos, quienes deben alertar a las personas correspondientes, cuando ocurre un hecho sospechoso.

Ilustración 2.13: Sistema cerrado de cámaras.

2.1.8. Sistema de seguridad con uso de aplicaciones móviles

El uso de los smartphones cada día se vuelve más importante e indispensable. Por esto, utilizar un sistema de control de acceso, a través de una aplicación móvil, disminuye el gasto total para el usuario final. Hoy, existen distintas aplicaciones para llevar a cabo esta tarea en diversos sistemas operativos como iOS y Android.

Dentro de las aplicaciones disponibles, se encuentran:

2.1.8.1. Sicon Mobile

Realiza un control de entrada y/o salida, identificando a los usuarios a través de tarjetas de accesos desarrolladas por Construred Servicios -empresa creadora de Sicon Mobile-. Las tarjetas son virtuales y cuentan con un código QR que es leído por dispositivos. [20]

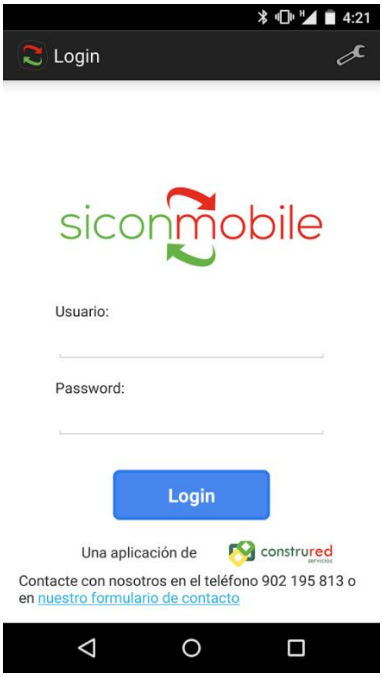


Ilustración 2.14: Primer vista aplicación SicomMobile

Ilustración 2.15: Vista tarjeta de presentación con código QR.

2.1.8.2. Safecard

Aplicación similar a la anterior, pero que adicionalmente cuenta con un servicio de invitaciones que poseen una validez durante el día y la hora indicados. Éstas se envían a través de un SMS, recibiendo un código numérico el cual se debe ingresar manualmente, o vía aplicación, recibiendo un código QR el cual se debe mostrar en los dispositivos de acceso al inmueble. [21] [22]

Ilustración 2.16: Vista principal aplicación SafeCard.

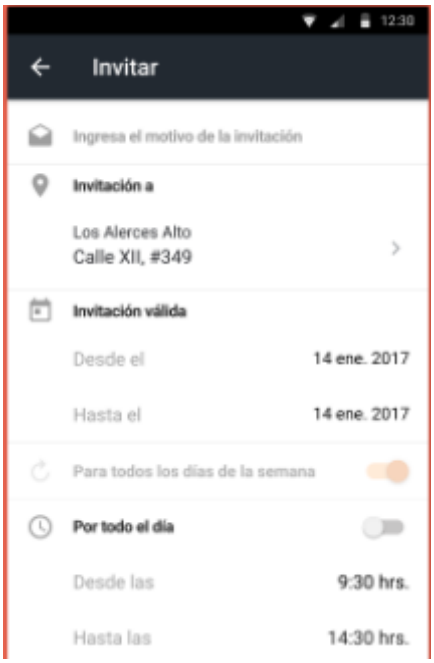


Ilustración 2.17: Generación de invitación aplicación SafeCard.

2.1.9. Sistema de seguridad por reconocimiento de iris

El iris es la membrana coloreada y circular del ojo, localizada detrás de la córnea. El iris posee la propiedad de una morfología aleatoria de su estructura.

El sistema de seguridad basado en iris es más flexible al momento de aplicar, por la facilidad de registrar la imagen a cierta distancia, sin necesidad de contacto físico. Un alto nivel de aleatoriedad en la estructura del iris permite 266° de libertad que pueden ser codificados y el iris es estable y sin cambios durante el periodo de vida. [23]

El proceso del sistema de reconocimiento de iris es el siguiente:

- Captura de la imagen: Se captura la imagen del iris, pudiendo ser obtenida hasta por tres cámaras con el fin de obtener una imagen más clara y con la mayor cantidad de detalles.
- Preprocesamiento de la imagen: Se aplican filtros que resalten los bordes del iris, pupilas y pestañas.
- Extracción zona de interés: Se extrae de la imagen el iris.
- Codificación: Se crea un histograma de la imagen y así obtener un valor que lo represente. Además, se localizan los centros y radios de la pupila e iris. Con los valores anteriores se codifica.
- Verificación: La verificación se realiza comparando la plantilla del individuo con la almacenada en la base de datos. Todas las comparaciones se realizan a través de una representación matemática obtenida. Si la verificación es correcta el sistema puede autorizar el ingreso al individuo. [24]

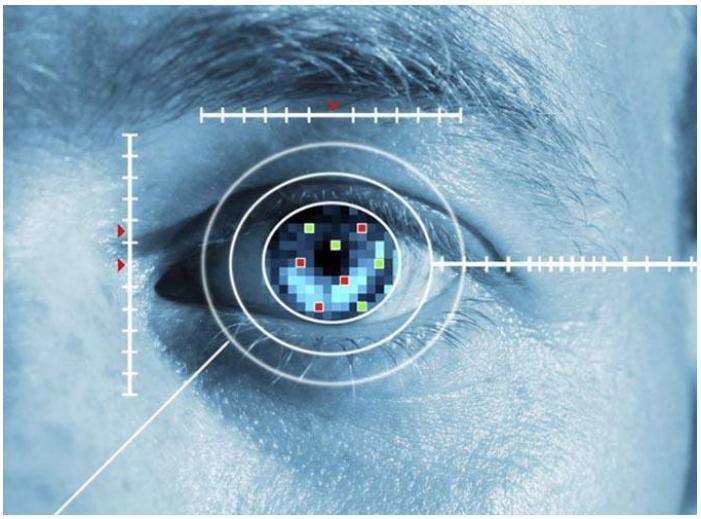


Ilustración 2.18: Reconocimiento de iris.

2.1.10. Sistema de seguridad tradicional, llave y conserje

El sistema de seguridad con control de acceso con llave personal y conserje es el más común y más vulnerable.

El sistema consta en que cada usuario posee una llave que le permite acceso al inmueble a través de la puerta principal y portón vehicular. Además, el conserje tiene un rol fundamental ya que es éste quien reconoce a los usuarios y les permite el acceso o, por el contrario, les prohíbe y exige identificación a los desconocidos o ajenos al lugar.

Ilustración 2.19: Conserje en su lugar de trabajo.

2.2. Sistema operativo Android

Android es el sistema operativo móvil más popular, basado en Linux y actualmente es utilizado desde teléfonos y relojes a automóviles y televisores. [25]

2.2.1 Historia de Android

Android Inc, fue fundada en Octuble del 2003, por Andy Rubin, Rich Miner. Chris White y Nick Sears, con el objetivo de desarrollar un sistema operativo para móviles.

Google compra Andoid Inc el 17 de Agosto del 2005. Esta compañía estuvo funcionando en forma secreta y se asumía que Google estaba planeando entrar al mercado de dispositivos móviles. Desde ese momento Google promete proveer un sistema flexible, escalable y focalizado en el usuario.

El 5 de Novimienbre del 2007 se crea Open Handset Alliance, una alianza liderada por Google con compañías tecnológicas como HTC, Dell, Intel, Motorola, Qualcomm, Texas Instruments, Samsung, LG, T-Mobile. Nvidia y Wind River System. [26]

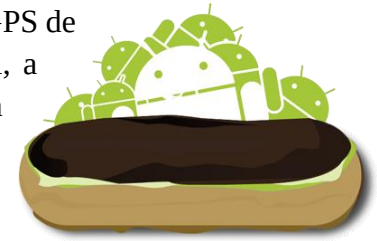
2.2.2 Evolución del sistema operativo Android

- Android 1.6: Donut

Se estableció como la primera versión reconocida de Android, que incluía cuadro de búsqueda rápida, diversidad de tamaños de pantallas, permitiendo la aparición de teléfonos móviles con pantallas con una resolución mayor a 320 x 480 -vertical- y la introducción de la plataforma Google Market, la cual ofrecía las principales aplicaciones pagadas y gratuitas. [26]

- Andoid 2.1 Eclair

Para esta versión de Android se integró la navegación de GPS de Google Maps, la personalización de la pantalla principal, a través de fondos animados soportados por pantallas con resolución de 854 x 480. Además, se integró un sistema de voz a texto, que permitía que con solo presionar el icono del micrófono se podían dar instrucciones al teléfono.



- Android 2.2 Froyo

Con Froyo llegaron los teléfonos de gran velocidad, gracias al compilador JIT a Dalvik y al motor V8 JavaScript. Las capacidades de hotspot de wifi garantizaron que los usuarios siempre tuvieran una conexión.

- Android 2.3 Gingerbread

Se creó la API de videojuegos, alcanzando gráficos en 3D. Se introdujo la compatibilidad con NFC y la opción de administrar el uso de la batería.

- Android 3.0 Honeycomb

Lo más relevante de este sistema operativo es la compatibilidad con el diseño de las tablets, barra del sistema y la configuración rápida.

- Android 4.0 Ice Cream Sandwich

En esta versión se permite la personalización de la pantalla principal a través de carpetas y bandejas de favoritos. Además, posee un control de uso de datos móviles y la creación de Android Bean, que permitió que dos teléfonos compartieran contenido de forma instantánea, mediante comunicación con NFC.

- Android 4.1 Jelly Bean

La inteligencia fue una de las facetas principales de Jelly Bean. Marcó el comienzo de la era de la asistencia móvil personalizada gracias a Google Now y a las múltiples cuentas que se podían configurar en el móvil.

- Android 4.4 KitKat

Permite realizar tareas con la voz, a través del comando “Ok Google” y posee un marcador inteligente priorizando los contactos más solicitados.

- Android 5.0 Lollipop

Permite las pantallas multiples sin interrupciones del teléfono a Tablet, el reloj Andoid Wear o Android TV. Además, se integran las notificaciones en la pantalla bloqueada.

- Android 6.0 Marshmallow
  Integra No won Tap, asistencia sin interrumpir las tareas. Además, se introduce la opción de permisos a las aplicaciones.

- Android 7.0 Nougat
  Ofrece funciones para mejorar el rendimiento, la productividad y la seguridad. [27]

Versión Android – Sistema Operativo	Nivel API	Distribución Acumulativa	Características
4.0 - Ice Cream Sandwich	15	97,4%	Compatibilidad con dispositivos Bluetooth Health Profile.
4.1 - Jelly Bean	18	95,2%	Admite grandes transferencias de carga útil a través de Bluetooth.
4.4 - KitKat	19	73,9%	Permite emular tarjetas NFC que permiten el intercambio de datos.
5.0 - Lollipop	22	40,5%	Permite interacción con dispositivos periféricos BLE.
6.0 - Marshmallow	23	4,7%	Escaneo de dispositivos Bluetooth Low Energy.

Tabla 2-1: Tabla comparativa entre distintos sistemas operativos Android.

2.2.3 Arquitectura

El sistema operativo Android es un stack de código abierto basado en Linux. En el siguiente diagrama se muestran los componentes principales de su arquitectura. [28]

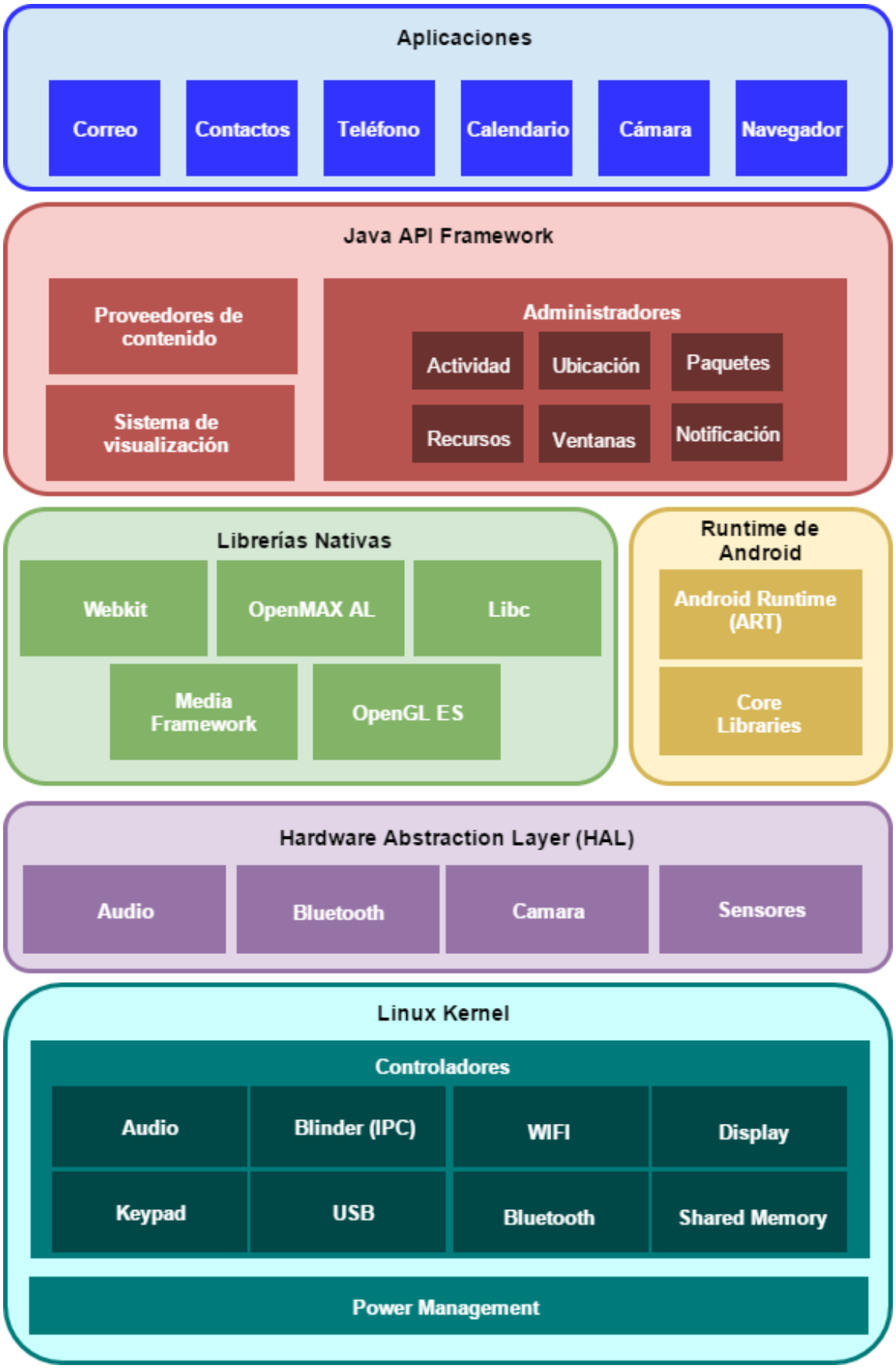


Ilustración 2.20: Arquitectura Sistema Operativo Android.

- Kernel de Linux
  La base de la plataforma Android es el kerne de Linux. Por ejemplo, el tiempo de ejecución de Android (ART) se basa en el kernel de Linux para funcionalidades subyacentes, como la generación de subprocesos y la administración de memoria de bajo nivel.
  Permite a los fabricantes de dispositivos desarrollar controladores de hardware para un kernel conocido.
  Además, esta capa contiene los drivers necesarios para que cualquier componente hardware pueda ser utilizado mediante las llamadas correspondientes, brindando portabilidad, flexibilidad y seguridad.

- Capa de abstracción de hardware (HAL)
  Brinda interfaces estándares que exponen las capacidades de harware del dispositivo al framework de la Java API de nivel más alto. HAL consistente en varios módulos de bibliotecas y cada uno de estos implementa una interfaz para un tipo específico de componente de hardware. Cuando el framework de una API realiza una llamada para acceder a hardware del dispositivo, el sistema Android carga el módulo de biblioteca para el componente de hardware en cuestión.

- Tiempo de ejecución de Android
  Para Android 5.0 o versiones superiores, cada aplicación ejecuta sus propios procesos con sus propias instancias del tiempo de ejecución de Android (ART). El ART permite ejecutar varias máquinas virtuales en dispositivos de memoria baja ejecutando archivos DEX, un formato de código de bytes diseñado especialmente para Android y optimizando para ocupar un espacio de memoria mínimo.
  Algunas de las funciones principales son la compilación ahead-of-time (AOT) y just-in-time (JIT), recolección de elementos no usados (GC) optimizada y mejor compatibilidad de depuración.

- Bibliotecas Nativas
  El código nativo que requiere bibliotecas nativas escritas en C y C++ es la base de muchos componentes y servicios centrales del sistema Android, como el ART y HAL.
  La plataforma Android proporciona la API del framework de Java para exponer la funcionalidad de algunas de estas bibliotecas nativas a las aplicaciones.

- Framework de Java API
  Las API escritas en el lenguaje Java proporcionan todas las funciones del sistema operativo Android. Estas API son la base que se necesita para crear

aplicaciones simplificando la reutilización de componentes del sistema y servicios centrales y modulares.
Algunos componentes son:

- Administrador de Actividades: Gestiona las activities de una aplicación y su ciclo de vida. Activity es cada una de las pantallas con las que el usuario interactúa.
  Además, proporciona una pila de retroceso de navegación común.
- Administrador de ventanas: Es el encargado de dirigir lo que se mostrará en pantalla.
- Administrador de recursos: Brinda acceso a recursos sin códigos, como strings localizados, gráficos y archivos de diseño.
- Administrador de notificaciones: Permite que todas las aplicaciones muestren alertas personalizadas en la barra de estado.
- Proveedores de contenido: Permite que las aplicaciones accedan a datos desde otras aplicaciones.

- Aplicaciones del sistema
  Algunas aplicaciones incluidas en Android son correo electrónico, mensajería, calendarios, navegación por internet y contactos, entre otros elementos.
  Además, las aplicaciones pueden ser accedidas y utilizadas por aplicaciones desarrolladas por los usuarios.

2.3. Tecnología Bluetooth

2.3.1 Introducción al Bluetooth

Bluetooth es una tecnología inalámbrica de corto alcance que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace de radiofrecuencia en la banda ISM de los 2.4 GHz.

Fue desarrollada en 1998 por Bluetooth SIG – Bluetooth Special Interest Group – alianza de los grandes grupos industriales Intel, Ericsson, IBM, Nokia y Toshiba.

Bluetooth es el protocolo de comunicaciones diseñado especialmente para dispositivos de bajo consumo, que requieran corto alcance de emisión y basados en transceptores de bajo costo.

Los dispositivos que cuentan con Bluetooth pueden comunicarse entre sí cuando se encuentran en el área de cobertura.

Para dispositivos móviles la potencia que utiliza Bluetooth son 2.5 mW o 4 dBm con un alcance máximo de 10 metros, lo que corresponde a clase 2. De acuerdo, a la

versión de Bluetooth es la capacidad de su ancho de banda. Las primeras versiones poseían un ancho de banda de 1 Mbit/s, en cambio, la versión 4, posee un ancho de banda de 32 Mbit/s. [29]

2.3.2 Bluetooth en el uso de aplicaciones móviles

La tecnología Bluetooth en el sistema operativo Android se ha ido implementando y desarrollando con cada versión de este.

El sistema operativo Android 4.0 Ice Cream Sandwich, API 15, fue el primero en implementar Bluetooth. Su uso era básico, no poseía identificación de dispositivos ni cifrado en la comunicación. A partir de las versiones posteriores, se comenzaron implementar cifrado en la transferencia de datos y seguridad en el momento de establecimiento de conexión.

Las primeras aplicaciones desarrolladas que utilizaban bluetooth permitían realizar conexiones entre dos dispositivos Android con el fin de intercambiar imágenes, videos y música.

Hoy, las aplicaciones que utilizan Bluetooth son muy diversas, debido que existen múltiples dispositivos con esta tecnología, algunas de ellas permiten realizar conexiones entre los smartphones y dispositivos de audio como equipos, parlantes y audífonos, periféricos como teclados, mouse y controles, vehículos, computadores, tablets, entre muchos otros. [30]

3. Capítulo: Análisis del estado del arte y comparación entre sistemas de seguridad implementados

En este capítulo se realizará un análisis del modo de operación de los sistemas de seguridad mencionados en el capítulo anterior. Además, se realizará una tabla comparativa entre las tecnologías mencionadas.

3.1. Análisis modo de operación sistemas de seguridad

Dentro de los sistemas de seguridad implementados alrededor del mundo y mencionados en el capítulo anterior, se puede apreciar cierta similitud en su forma de operar, lo que se representará en el siguiente diagrama.

Tabla 3-1: Diagrama ejemplificador del funcionamiento de los sistemas de seguridad.

Fuente: Elaboración propia.

El diagrama anterior resume cómo funcionan los sistemas de seguridad o de control de acceso implementados y permiten un acercamiento a la solución.

Del diagrama se pueden obtener los módulos principales para la creación del sistema de seguridad. Estos son:

- Módulo de entrada:
  Dentro de este módulo se encuentra todo lo que concierne a la captura de datos del sistema con el usuario, como cámaras, llaves, identificadores, teclados, entre otros.

- Módulo de comunicación:
  Aquí se encuentra la tecnología de comunicación a utilizar, los emisores y receptores del mensaje.

- Módulo de procesamiento:
  En el módulo de procesamiento se espera identificar el hardware y software necesario para procesar la información obtenida desde la entrada y emitir una salida.

- Módulo de salida
  Dentro de la salida se considera todo tipo de interacción para hacer saber al usuario si su petición fue permitida o denegada.

3.2. Comparación entre sistemas de seguridad implementados

Se explicará mediante una tabla comparativa las diferencias entre algunas tecnologías mencionadas en el capítulo anterior. Además, se integrará el Bluetooth.

Tecnología	Invasivo	Medio de Acceso	Autonomía	Radio de operación	Lenguaje Recomendado
NFC	Moderado	NFC Card	Sin consumo energético	Por contacto	Java
RFID Activo	Nulo	Smartphone, RFID tag.	Depende del Smartphone	< 10 metros	Java
Bluetooth	Bajo	Smartphone, tag.	Depende del Smartphone	< 10 metros	Java

Tabla 3-2: Tabla comparativa de tecnologías

Fuente: Elaboración propia.

Se consideraron las tecnologías anteriores, ya que estas cuentan con el requerimiento del cliente de ser no invasivas. En el siguiente capítulo se detallarán los requerimientos.

4. Capítulo: Identificación de elementos claves y selección de tecnologías

En este capítulo se identificarán los principales elementos que se deben tener en consideración para la selección de tecnología, con el fin de encontrar la solución óptima.

4.1. Puntos de interés

A continuación, se detallan algunos puntos relevantes que deben ser considerados para poder realizar la selección de tecnologías y desarrollar la solución.

4.1.1. Cliente – Contraparte

La inmobiliaria Fundamenta ocupa un rol fundamental en el desarrollo de este proyecto. Es por ello que es necesario considerar algunos aspectos como la ubicación de los edificios, los usuarios, sus exigencias, entre otros.

Unos de los principales requerimientos por parte de la inmobiliaria es que el sistema a desarrollar sea “no invasivo”. Con esto se quiere decir, que los tiempos de acceso al inmueble de todo usuario sea el menor posible, por lo que es necesario considerar periodos cortos de identificación, validación y creación de perfiles.

Otro de los requerimientos establecidos por parte de la contraparte es brindar seguridad entre pisos. Debido a que durante los últimos años es común encontrar a personas que arriendan departamentos con el fin de robar a sus vecinos.

Además, el cliente exige el uso de smartphone y la tecnología Bluetooth.

4.1.2. Usuarios

Este ítem está considerado para clasificar y describir los usuarios que utilizarán el sistema a proponer, los que finalmente se transformarán en el público objetivo de este proyecto.

Según datos entregados por la contraparte, el público promedio que vive en sus inmuebles son personas entre 25 y 45 años, de clase social media aspiracional.

Considerando que el desafío es planteado para proyectos habitacionales de gran envergadura, se consideran en una primera fase, dos tipos de usuarios, los cuales se han clasificado según el tipo de interacción con el sistema. Estos son:

- Usuario tipo I
  En esta categoría se encuentran los usuarios estándar del sistema, aquellos que solo interactúan a través del dispositivo de acceso. No deben poseer un conocimiento previo acabado, ya que solo emitirán peticiones, que el sistema debe procesar.
- Usuario tipo II
  En esta categoría se encuentran los usuarios que deben tener un conocimiento previo del sistema, ya que estos son los encargados de registrar a todas las personas nuevas que desean ingresar al inmueble y explicarles cómo funciona el dispositivo. Aquí se encuentran los conserjes.

Como se menciona anteriormente, los usuarios tipo II del sistema son los conserjes, quienes serán los encargados de mantener el sistema en marcha y de explicarles a los demás usuarios cómo funciona el sistema, por lo que este debe ser simple de utilizar y mantener.

También, es importante recalcar que los conserjes no son los únicos trabajadores que se pueden encontrar en los edificios. También, puede haber personal de aseo, jardineros, de tiempo completo o parcial, por lo que es importante clasificar el nivel de acceso que tendrán los usuarios y el tiempo de validez de este.

Un punto importante a considerar, son las visitas, para las cuales se consideran tiempos de validez y rutas establecidas.

Por lo anterior, es necesario contar una segunda fase de clasificación, según el nivel de acceso.

Tipo usuario	Nivel de acceso	Periodo validez	Rango de Acceso
Conserje	3	Indefinido	Total
Habitantes	3	Indefinido	Total
Visitas	1	Diario	Parcial
Repartidores (comida rápida, despacho muebles)	1	Diario	Parcial
Personal de Aseo	2	Indefinido	Parcial
Jardineros	2	Indefinido	Parcial
Maestros ocasionales	1	Diario	Parcial

Tabla 4-1: Distintos tipos de usuarios.

Fuente: Elaboración propia.

De acuerdo con la tabla anterior, se posee tres niveles de acceso, los que se detallarán a continuación.

- Nivel de acceso 1
  Es el nivel con más restricciones, el cual consta de un pase temporal y acceso parcial, aquí se encuentran las visitas, repartidores y trabajadores ocasionales.
  Los usuarios que posean esta clasificación no contarán con acceso al portón vehicular y la duración de su pase será de 10 horas.

- Nivel de acceso 2
  Es el nivel intermedio, el cual consta de un pase indefinido y acceso parcial. Aquí se encuentran los trabajadores del inmueble o de los departamentos.
  Los usuarios que posean esta clasificación no contarán con acceso al portón vehicular y la duración del pase será indefinido.

- Nivel de acceso 3
  Es el nivel con más privilegios, el cual consta de un pase indefinido que solo será eliminado por el conserje o administrador y acceso total a todo el inmueble. En esta sección se encuentran los habitantes del edificio y los conserjes.

4.1.3. Seguridad y ambiente

Dentro de este ítem se debe considerar que los inmuebles de la inmobiliaria son del tipo eco-amigables, por lo que cualquier intervención debe seguir en la misma línea, utilizando, por ejemplo, componentes de bajo consumo energético.

Otro factor importante es la ornamentación del edificio, por lo que el sistema a desarrollar debe mimetizarse con el ambiente.

Los edificios de la inmobiliaria Fundamenta son, en su gran mayoría, de 20 o más pisos por lo que cualquier sistema de seguridad debe poder controlar grandes flujos de personas.

Además, las ubicaciones de estos son en zonas muy transcurridas y centrales de Santiago, lo que vuelve necesario e importante que el sistema a crear sea rápido, eficaz y robusto.

Por último, la gran oferta de departamentos en las zonas aledañas hace que la competencia sea dura, por lo que la inmobiliaria busca diferenciarse de sus rivales, a través de la tecnología y la seguridad.

4.2. Selección de tecnologías

De acuerdo con lo visto anteriormente, la tecnología de comunicación a utilizar debe ser inalámbrica y debe funcionar en un dispositivo smartphone.

El ingreso de nuevos usuarios será realizado por el conserje, por lo que las interfaces deben ser de fácil uso.

Todos los sistemas anteriormente nombrados, funcionan con una base de datos, en la cual se ingresan los usuarios y sus características, por lo que es necesario contar con ello.

La base de datos y el procesamiento de esta y de las acciones a tomar por el sistema deben ser alojados en algún hardware pequeño, que no sea llamativo para ladrones, por lo que micro computadores o procesadores son una clara opción.

Considerando que la mayoría de las personas posee Smartphone con Android, será este el sistema operativo seleccionado para encontrar la solución.

5. Capítulo: Análisis de Requerimientos y acercamiento de la solución

En el desafío propuesto, hay una variedad de restricciones que imponen requerimientos mínimos en el sistema de seguridad a implementar. En este capítulo se identificarán los elementos relevantes y se detallarán los requerimientos de este.

5.1. Requisitos del sistema

5.1.1. Requisitos funcionales del sistema

Los requerimientos funcionales son obtenidos de acuerdo al análisis del estado del arte y de las exigencias del cliente. Dentro de los requisitos funcionales se encuentran:

1. El sistema debe contar como tecnología principal Bluetooth.
2. El sistema debe ser utilizado a través de smartphones.
3. Debe poseer un sistema de registro de todos los usuarios.
4. Debe poseer un sistema de login.
5. Debe permitir o denegar el acceso según usuario.
6. Mantener un registro de los usuarios que hagan uso del sistema.
7. Alertar cuando un individuo no autorizado solicite ingresar.
8. El dispositivo Android del usuario debe ser capaz de emparejarse al sistema.
9. El sistema debe interpretar los datos obtenidos desde la aplicación del Smatphones.
10. La aplicación del Smatphone debe lograr enviar datos a través del Bluetooth.

5.1.2. Requisitos no funcionales del sistema

Dentro de los requerimientos no funcionales se encuentran:

1. Controlar altos flujos de personas que ingresan al inmueble.
2. El sistema debe ser robusto.
3. El sistema no debe ser invasivo.
4. Ser simple de utilizar.
5. Control de accesos a pisos del edificio.

5.2. Requisitos de Ambiente

5.2.1. Hardware

Para el desarrollo de la aplicación se utilizará Android Studio, por lo que el computador debe poseer un procesador Intel Core i5, Ram mínima de 8 GB y virtualización.

Para la ejecución de la aplicación se requiere un smartphone con sistema operativo Android 4.0.3 o superior que posea Bluetooth.

5.3. Módulos

En esta sección se detallarán los módulos a implementar.

Tabla 5-1: Módulos que componen el sistema.

Fuente: Elaboración propia.

5.3.1. Entrada

Se define como la primera interacción con el sistema, la parte visible con la cual se interactuará para poder hacer ingreso al edificio e inscribir, modificar y eliminar usuarios y/o permisos.

En este módulo se encuentra la aplicación del usuario, el uso de cámaras, teclados, smartphones.

- Cámara: su función es capturar la imagen del usuario al momento de ser ingresado al sistema.
- Teclado: su función es ingresar los datos alfanuméricos al sistema de los nuevos usuarios y los visitantes, dentro de estos datos se consideran indispensables, el piso, departamento, nombre, MAC del smartphone y clasificación.
- Aplicación en el smartphone: su deber es mandar peticiones al sistema, para solicitar acceso o ascensor.
- Pantalla conserje: es la encargada de contener la interfaz de interacción del conserje, capaz de ingresar, editar y eliminar a usuarios del sistema.

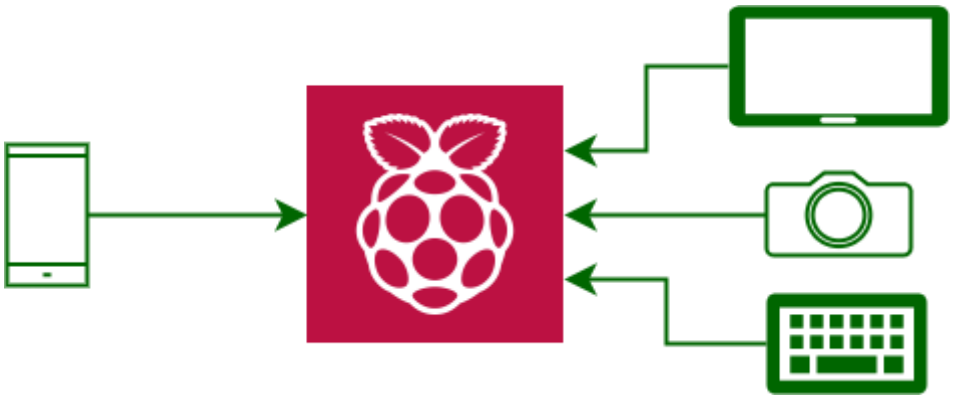


Tabla 5-2: Módulo entrada.

Fuente: Elaboración propia.

5.3.2. Comunicación

Como módulo de comunicación se considera la tecnología inalámbrica a aplicar, el encargado de esta tarea es Bluetooth a través de una aplicación móvil, la que permitirá al usuario solicitar ascensor al piso deseado o solicitar el desbloqueo de una puerta.

Al momento de hacer ingreso del usuario al sistema se debe emparejar el dispositivo inteligente con el servidor utilizado, autentificando esta operación por medio de un código. Además, la MAC del dispositivo será integrado al sistema en

la base de datos, para cuando se realicen peticiones, el sistema sea capaz de verificar al usuario a través de esta.

La aplicación opera sobre la plataforma Android y está disponible su uso solo dentro del rango de cobertura del Bluetooth.

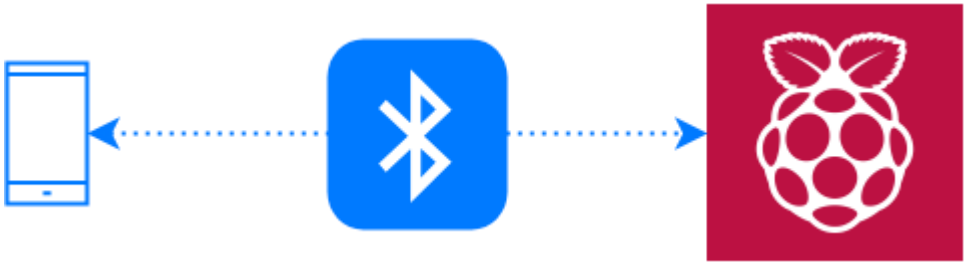


Tabla 5-3: Módulo de comunicación.

Fuente: Elaboración propia.

5.3.3. Procesamiento

Para el procesamiento de datos, se utiliza un Raspberry Pi 3, modelo B, es un CPU de tamaño reducido, que permite su interconexión con diversos dispositivos, como teclados, cámaras o cualquiera con conexión USB.

Una de sus mayores características es el bluetooth integrado, por lo que no es necesario contar con un módulo anexo.

En él, se monta la base de datos y se ejecuta un programa de diseño propio, el cual se encarga de capturar todos los datos de las fuentes de comunicación, procesarlos y responder las solicitudes, ya sea, abrir una puerta, denegar acceso, permitir el movimiento del ascensor, entre otras.

Además, la Raspberry debe contener un módulo web que permita al conserje interactuar con ella.

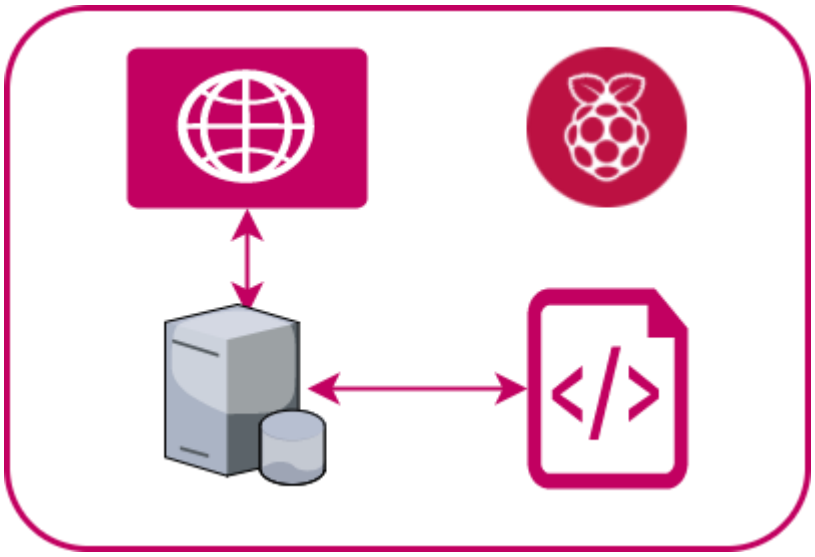


Tabla 5-4: Módulo de procesamiento.

Fuente: Elaboración propia.

5.3.4. Salida

En el módulo de salida se considera todo tipo de respuesta que genere el sistema. Estas son:

- Pantalla conserje: es la encargada de mostrar el estado del sistema, como usuarios registrados, frecuencia de acceso, advertencias y modo de funcionamiento.
- Pantalla usuario final: es la encargada de mostrar el estado de la solicitud del usuario como ingreso denegado, usuario sin permiso o ascensor en camino.
- Actuadores: están ubicados en el ascensor, en la entrada principal y en la entrada vehicular, se accionan a través de señales enviadas por el microcomputador.

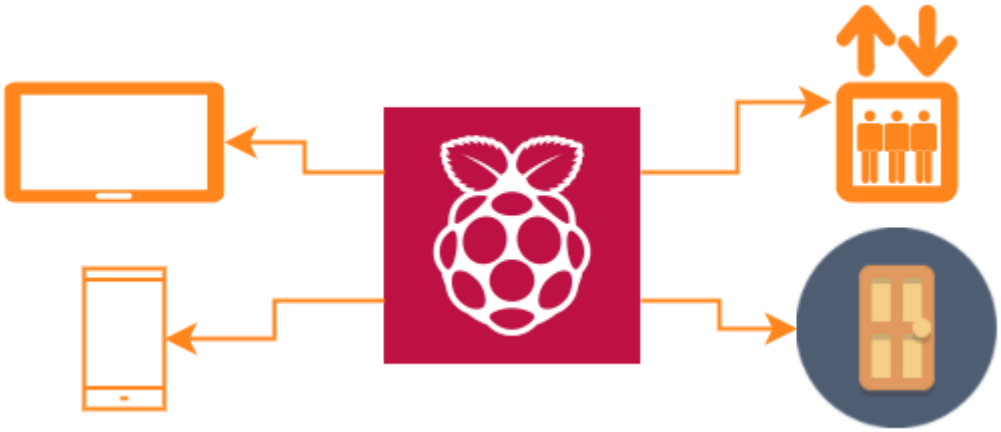


Tabla 5-5: Módulo de salida.

Fuente: Elaboración propia.

5.4. Matriz de requisitos funcionales y módulos

RF \ Módulos	Entrada	Comunicación	Procesamiento	Salida
RF1		**x**		
RF2	**x**			**x**
RF3			**x**	
RF4	**x**			
RF5				**x**
RF6			**x**	
RF7				**x**
RF8		**x**		
RF9			**x**	
RF10	**x**	**x**		

Tabla 5-6: Matriz de requisitos funcionales y módulos.

Fuente: Elaboración propia.

RF1 El sistema debe contar como tecnología principal Bluetooth.

RF2 El sistema debe ser utilizado a través de smartphones.

RF3 Debe poseer un sistema de registro de todos los usuarios.

RF4 Debe poseer un sistema de login.

RF5 Debe permitir o denegar el acceso según usuario.

RF6 Mantener un registro de los usuarios que hagan uso del sistema.

RF7 Alertar cuando un individuo no autorizado solicite ingresar.

RF8 El dispositivo Android del usuario debe ser capaz de emparejarse al sistema.

RF9 El sistema debe interpretar los datos obtenidos desde la aplicación de los smartphones.

RF10 La aplicación del smartphone debe lograr enviar datos a través del Bluetooth.

6. Capítulo: Diseño y desarrollo de la solución

6.1. Esquemas

En esta sección se presentarán algunos esquemas para entendimiento del lector sobre el planteamiento de la solución y algunos diagramas necesarios para el desarrollo de esta.

6.1.1 Diagrama de arquitectura

En la siguiente figura se muestra el principal flujo de información por el todo el sistema.

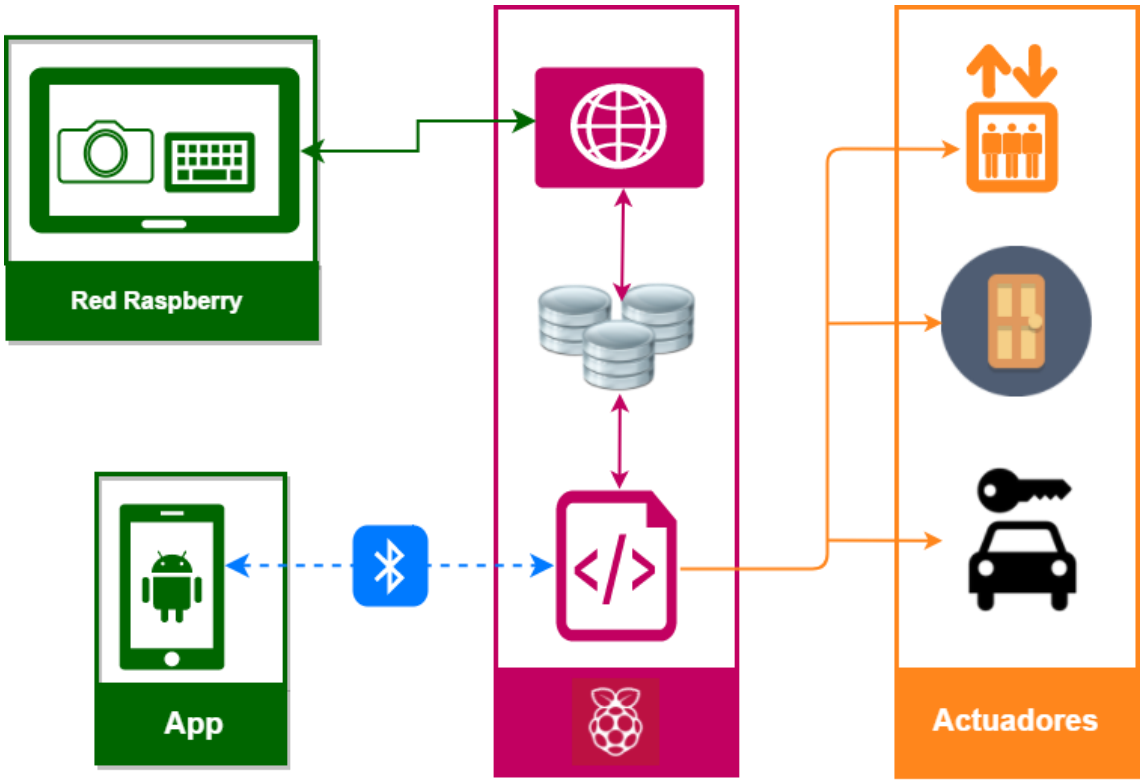


Ilustración 6.1: Diagrama de arquitectura.

Fuente: Elaboración propia.

6.1.2 Diagrama de flujo funcionamiento del sistema

El diagrama presentado en esta sección representa a grandes rasgos el modo de funcionamiento del sistema.

Cuando el usuario ingresa por primera vez al inmueble y no posee la aplicación para el smartphone personal, debe pasar por conserjería e identificarse. El conserje toma los datos del usuario y lo ingresa al sistema, a la base de datos. Además, le proporciona la aplicación móvil al usuario y empareja el dispositivo smartphone al sistema.

Una vez ingresado el usuario a la plataforma, el sistema, de acuerdo a los datos ingresados, clasifica al usuario según su nivel de acceso.

Si el usuario se encuentra dentro del área de cobertura del Bluetooth ya está habilitado para hacer uso del sistema y, a través de la aplicación móvil puede requerir acceso a la puerta principal, al portón vehicular o solicitar al ascensor al piso en el que se encuentra.

Una vez generada la petición de parte del usuario, el sistema es el encargado de verificar los permisos de accesos y tiempo de disponibilidad de éste, en caso de cumplirlos se valida la petición y el sistema responde con la acción acordada por el usuario. Por el contrario, si el usuario no cuenta con los permisos, el sistema niega el acceso o la petición y se lo hace saber al usuario a través de un mensaje en sus dispositivos móvil.

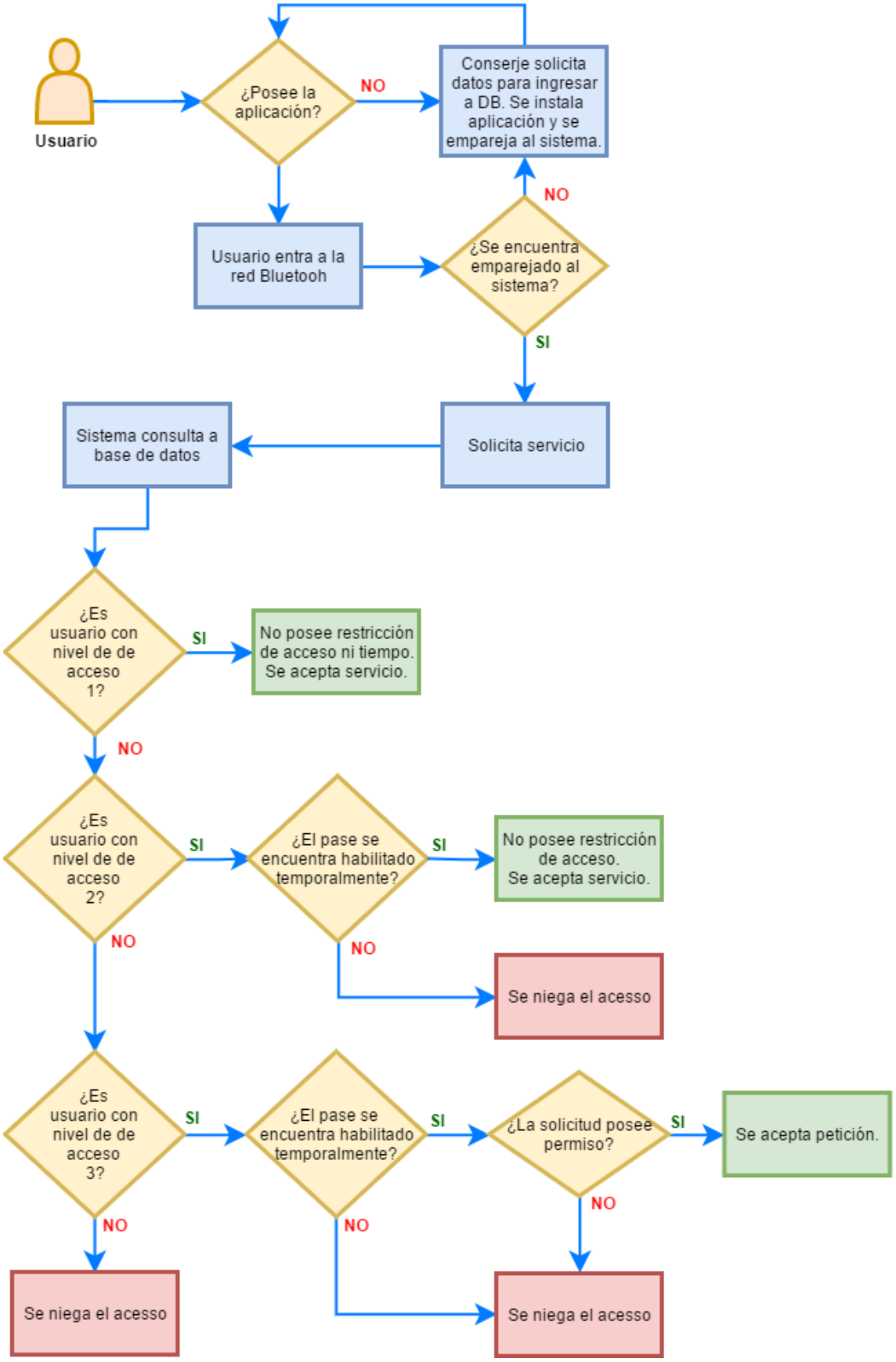


Ilustración 6.2: Diagrama de flujo.

Fuente: Elaboración propia.

6.1.3 Modelo de casos de uso

El siguiente modelo representa, a grandes rasgos, la funcionalidad del sistema de seguridad a desarrollar y los distintos actores involucrados.

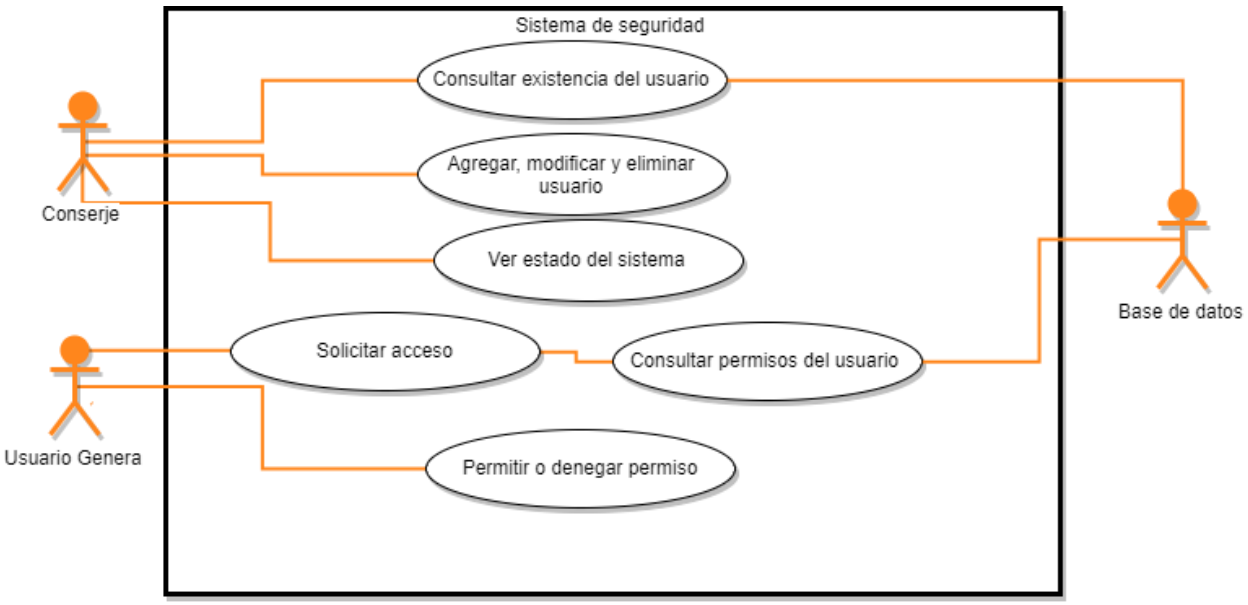


Ilustración 6.3: Modelo casos de usos.

Fuente: Elaboración propia.

6.2. Trabajo Previo

En esta sección se describirá la preparación y las herramientas utilizadas para la creación de la solución.

6.2.1 Preparación Raspberry Pi 3

El microcomputador Raspberry Pi 3 modelo B, es el utilizado para alojar la base de datos y los programas capaces de realizar el intercambio de información entre el exterior y la base de datos. Además, es el encargado de emitir respuestas a las peticiones de los usuarios.

Para describir la preparación de la Raspberry Pi, se dividirá en sub-módulos.

6.2.1.1 Sistema Operativo

Para la elección del sistema operativo, se debe tener en cuenta que la Raspberry cumple con el objetivo de servidor y computador.

El sistema operativo más recomendado para este uso es Raspbian Debian Jessie.

Raspbian es un sistema operativo libre basado en Debian optimizado para el hardware Raspberry, posee más de 35000 paquetes, contiene herramientas de desarrollo como IDLE para el lenguaje de programación en Python y está optimizado para procesadores ARM de bajo rendimiento de la línea Raspberry Pi.

Instalación

Para la instalación del sistema operativo se necesita un micro SD de 4 GB o superior. Se recomienda utilizar NOOBS, New Out Of Box Software, que es un instalador sencillo de sistemas operativos. Se necesita contar con la imagen de Raspbian en formato .img, la cual se graba en la micro SD.

En la Raspberry se debe escoger el sistema operativo a instalar, en este caso, Raspbian.

Ilustración 6.4: Captura instalación sistema operativo.

6.2.1.2 Base de datos

El motor de la base de datos se encuentra a cargo de MariaDB. MariaDB Server es realizado por los desarrolladores de MySQL y garantizado para permanecer en código abierto.

Se utiliza por la rapidez, escalabilidad y robustez que posee.

MariaDB se desarrolla como una base de datos relacional que proporciona una interfaz SQL para el acceso de datos. Además, se puede incluir características GIS y JSON.

Instalación

En la consola se ingresa: *sudo apt-get install mariadb-server*

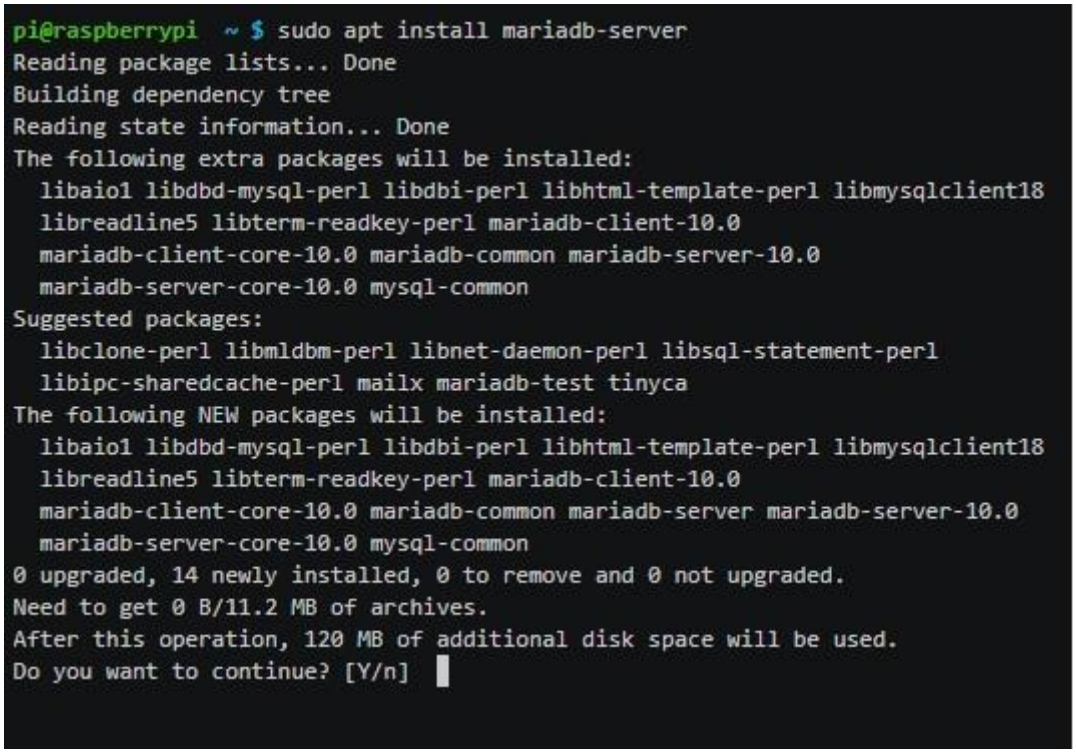


Ilustración 6.5: instalación MariaDB

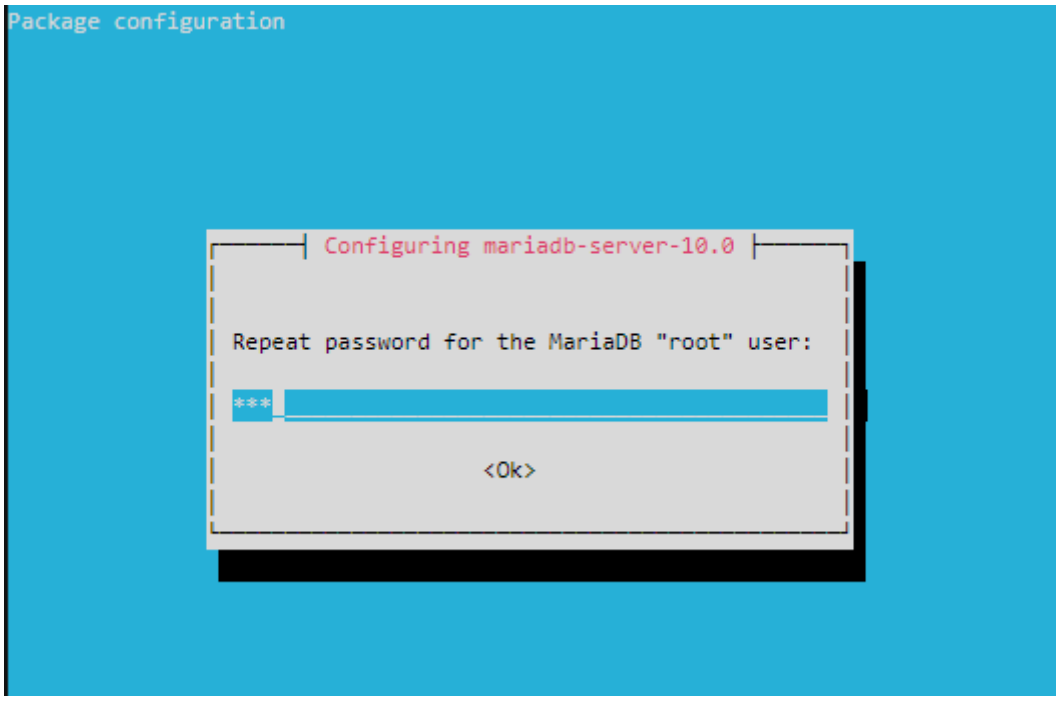


Ilustración 6.6: Instalación MariaDB contraseña.

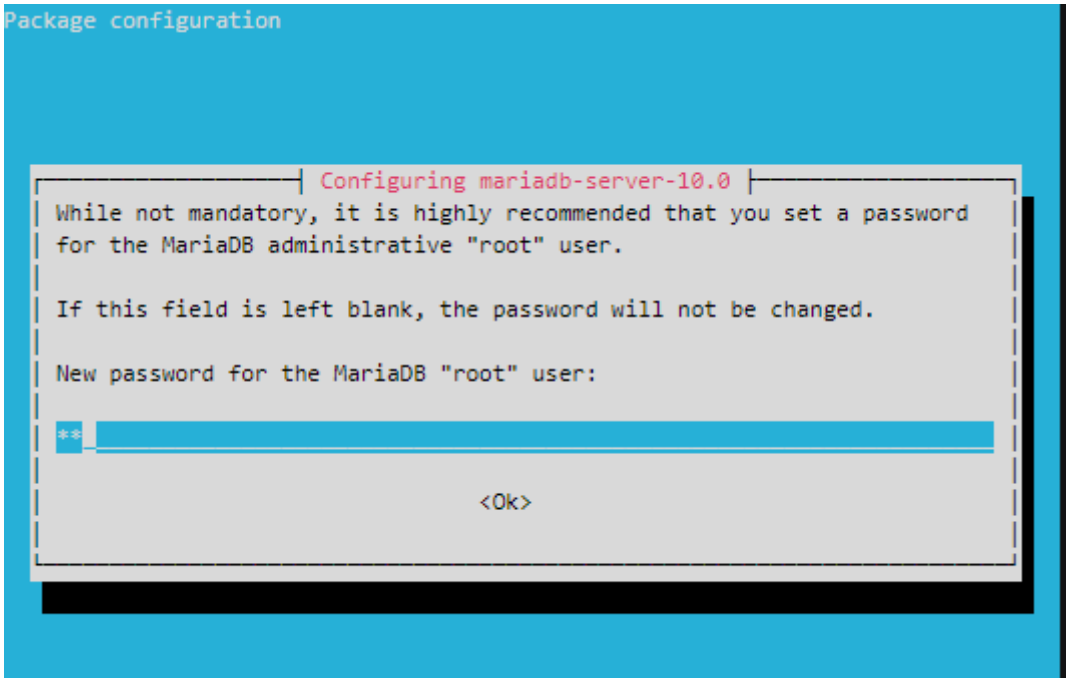


Ilustración 6.7: Instalación MariaDB contraseña root.

Se introducen contraseñas.

6.2.1.3 Lenguaje de programación

Para el lenguaje de programación se utiliza Python en Raspberry.

Python ya se encuentra instalado en Raspbian, por lo que es necesario complementarlo con bibliotecas de acceso a base de datos y a las salidas de la Raspberry GPIO.

Se instalan las herramientas de desarrollo para construir módulos en Python.

```
pi@raspberrypi  ~ $  sudo apt-get install python-dev
```

Instalación de API mysql, totalmente compatible con MariaDB.

```
pi@raspberrypi  ~ $  sudo apt-get install python-mysql
```

Instalación biblioteca Rpi.GPIO, la cual contiene la administración de los pines de entrada y salida de la Raspberry.

```
pi@raspberrypi  ~ $  sudo apt-get install rpi.gpio
```

Además, se debe instalar bluez, la cual es una biblioteca de Python para sistemas Windows y GNU/Linux.

6.2.1.4 Complementos

Se considera instalar algunos paquetes extras para habilitar conexión a un servidor que entregue la hora, dado que la Raspberry no posee hora local, debido a la inexistencia de pila, y el servicio SMTP para enviar correos en caso de alertas.

Hora

```
pi@raspberrypi  ~ $  sudo apt-get install ntp
pi@raspberrypi  ~ $  sudo nano /etc/ntp.conf
```

Dentro del archivo se ingresan el servidor que nos proporcionará el horario.

Correo

```
pi@raspberrypi  ~ $  sudo apt-get install ssmtp
pi@raspberrypi  ~ $  sudo apt-get install mailutils
pi@raspberrypi  ~ $  sudo nano /etc/ssmtp/ssmtp.conf
```

Configuración del archivo ssmtp.conf

```
root = postmaster
mailhub = smtp.gmil.com:587
hostname = raspberrypi
AuthUser =
AuthPass =
FromLineOverride = YES
UseSTARTTLS = YES
```

La configuración anterior es para asociar un correo Gmail, en AuthUser se debe completar con el nombre de usuario o correo electrónico y para AuthPass se debe completar con la contraseña asociada al usuario.

6.2.2 Preparación aplicación móvil

Para la creación de la aplicación móvil se deberá instalar Android Studio.

Instrucciones

- Se descarga Android Studio de la página oficial.
- Se ejecuta el archivo .exe
- Se debe configurar una variable de entorno que indique la ubicación de destino de instalación JDK.

7. Capítulo: Programación

En este módulo se mencionarán las funciones, algoritmos y toda la información relevante de la programación en Python sobre la Raspberry y en Android para la aplicación móvil.

7.1. Programación en Raspberry

La programación en Raspberry se dividirá en dos grupos: el código en Python y la creación de la base de datos en MariaDB.

7.1.1 Programa Python

El programa en Python debe procesar las entradas producidas por la aplicación móvil a través de Bluetooth, consultar a la base de datos y emitir una respuesta, la cual debe ser dirigida a la aplicación y a los actuadores conectados a la Raspberry.

7.1.1.1 Captura de entradas

Para que el sistema sea capaz de capturar entradas recibidas vía Bluetooth se debe importar la biblioteca bluetooth.

```
from bluetooth import *
```

Servicio RFCOMM

Es un conjunto simple de protocolos de transporte que proporciona conexiones simultáneas para dispositivos bluetooth.
RFCOMM genera puertos virtuales por los cuales se vinculan las conexiones mediante Bluetooth.
Un proceso actúa como servidor que acepta las conexiones y otro proceso actúa como cliente que solicita conexión.

SDP

SDP es un protocolo de descubrimiento de servicios para buscar y anunciar conexiones bluetooth.
El SDP de bluetooth define una forma de representar un rango UUID - identificador único universal de 128 bits – de una forma más corta.
El UUID identifica un servicio que está disponible en un dispositivo en particular.

El siguiente código anuncia un servicio, donde el nombre del servicio es "MMFundamenta" con un identificador único.

```
uuid = "94f39d29-7d6d-437d-973b-fba39e49d4ee"

advertise_service( server_sock, "MMFundamenta",
                   service_id = uuid,
                   service_classes = [ uuid, SERIAL_PORT_CLASS ],
                   profiles = [ SERIAL_PORT_PROFILE ],
                   protocols = [ OBEX_UUID ]
                    )
```

OBEX es un protocolo de comunicaciones que facilita el intercambio de objetos binarios entre dispositivos y se encuentra implementado sobre RFCOMM.

Las funciones principales que se utilizan se detallan en la siguiente tabla.

Función	Descripción
Server_sock = BluetoothSocket (RFCOMM)	Construcción socket servicio RFCOMM
server_sock.bind(("",PORT_ANY))	Servidor enlaza secuencia de comandos en el host " " por cualquier puerto.
Server_sock.listen()	Servidor escucha y acepta conexión.
port = server_sock.getsockname()[1]	Obtiene número del puerto.
client_sock, client_info = server_sock.accept()	Se acepta la solicitud de conexión, se obtiene el socket utilizado para la comunicación con el cliente y su información. Dentro de la información se encuentra la MAC del dispositivo.
data = client_sock.recv(1024)	Se reciben los datos enviados por el cliente, con un máximo de 1024 caracteres.
client_sock.send(data)	Se envían datos al cliente.
client_sock.close()	Se cierra conexión de socket cliente.
server_sock.close()	Se cierra conexión de socket sevidor.

Tabla 7-1: Funciones principales en Python para Bluetooth.

7.1.1.2 Consulta base de datos

Para que el sistema sea capaz de conectarse a la base de datos se importa MySQLdb, el cual es compatible con la base de datos MariaDB.

```
import MySQLdb
```

Las funciones principales se detallarán en la siguiente tabla.

Función	Descripción
conn = MySQLdb.connect()	Realiza conexión a la base de datos.
Con.cursor()	Genera un cursor.
Cursor.execute(consulta)	Encargado de ejecutar la consulta.
Cursor.fetchone()	Lee solo un registro de la respuesta de la consulta.
Cursor.close()	Se cierra el cursor
Con.close()	Se cierra conexión
Cursor.fetchall()	Recibe todas las respuestas de la consulta.

Tabla 7-2: Funciones principales en Python para conexión base de datos.

7.1.1.3 Salida

En este módulo se explica como el programa genera las salidas a través de los pines de la Raspberry, los cuales deben ser conectados a los distintos actuadores como la puerta principal, el portón vehicular y el ascensor.

Lo primero que se debe hacer es setear los pines como BCM.

La opción BCM significa que se está refiriendo a los pines por el número Broadcom SOC channel.

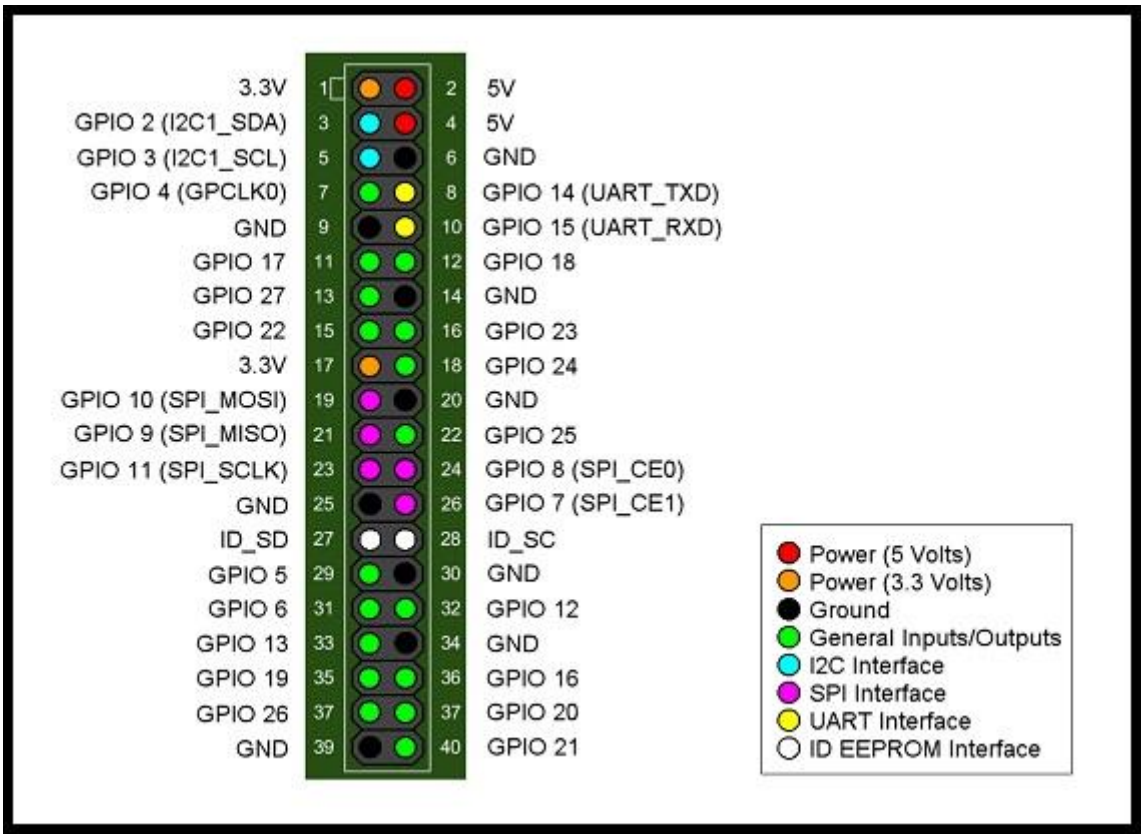


Ilustración 7.1: Pines GPIO salida de Raspberry Pi 3 Modelo B.

```
import RPi.GPIO as GPIO

os.system('modprobe w1-gpio')

GPIO.setmode(GPIO.BCM)
GPIO.setup(17, GPIO.OUT)
GPIO.setup(18, GPIO.OUT)
GPIO.setup(21, GPIO.OUT)
GPIO.setup(22, GPIO.OUT)
GPIO.setup(23, GPIO.OUT)

 GPIO.output(17, GPIO.HIGH)
 time.sleep(1)
 GPIO.output(17,GPIO.LOW)
```

Las funciones se explican a continuación.

Función	Descripción
GPIO.setmode(GPIO.BCM)	Se configuran los pines a BCM.
GPIO.setup(17, GPIO.OUT)	Se configura el pin en BCM 17 como salida.
GPIO.output(17, GPIO.HIGH)	Se emite una salida, subiendo el voltaje.
GPIO.output(GPIO.LOW)	Se emite una salida, disminuyendo el voltaje.

Tabla 7-3: Funciones principales utilizadas en Python para manipulación de pines.

7.1.2 Base de datos

En este módulo se presentarán las distintas tablas y relaciones del modelo de base de datos.

7.1.1.1 Tablas

Dentro de la base de datos existen cinco tablas, las cuales se describirán a continuación.

- **Permiso**

Nombre del campo	Tipo de dato	Descripción
MAC	CHAR(17)	MAC del dispositivo asociado al sistema de seguridad
RUT	VARCHAR(10)	RUT de la persona asociado al dispositivo.
NIVEL	INT(1)	Nivel de acceso que posee el dispositivo

Tabla 7-4: Base de datos - Tabla Permiso.

- **Personal**

Nombre del campo	Tipo de dato	Descripción
RUN	VARCHAR(10)	RUN de la persona.
NOMBRE	CHAR(12)	Nombre de la persona
APELLIDOP	CHAR(12)	Apellido paterno de la persona.
APELLIDOM	CHAR(12)	Apellido materno de la persona.
TELEFONO	INT(11)	Teléfono de la persona.
TIPO	CHAR(10)	Clasificación de los usuarios: Trabajador, Residente, Invitado.

Tabla 7-5: Base de datos - Tabla Personal.

- **Trabajador**

Nombre del campo	Tipo de dato	Descripción
RUN	VARCHAR(10)	RUN del trabajador asociado al sistema
CARGO	CHAR(20)	Cargo del trabajador
CORREO	CHAR(50)	Correo electrónico del trabajador.

Tabla 7-6: : Base de datos - Tabla Trabajador.

- **Residente**

Nombre del campo	Tipo de dato	Descripción
RUN	VARCHAR(10)	RUN del residente.
DEPARTAMENTO	VARCHAR(6)	Departamento donde habita el residente.
CORREO	CHAR(50)	Correo electrónico del residente.
PISO	INT(2)	Piso del departamento del residente.

Tabla 7-7: : Base de datos - Tabla Residente.

- **Invitados**

Nombre del campo	Tipo de dato	Descripción
RUN	VARCHAR(10)	RUN del invitado.
DEPARTAMENTO	VARCHAR(6)	Departamento al cual el invitado asiste.
FECHA	DATETIME	Fecha y hora de ingreso del invitado.

Tabla 7-8: : Base de datos - Tabla Invitados.

7.1.1.2 Relaciones

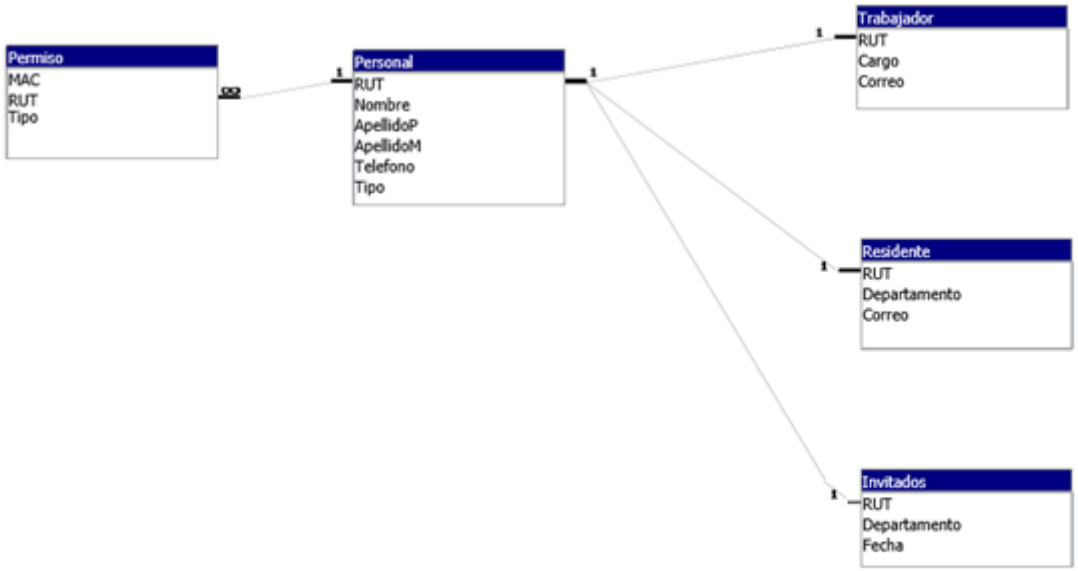


Ilustración 7.2: Base de datos.

7.2. Programación aplicación móvil

Para gestionar la funcionalidad de Bluetooth, se utiliza android.bluetooth, quien proporciona las clases que permiten conectarse con dispositivos y administrar la transferencia de datos entre estos. La API de Bluetooth admite tanto Classic Bluetooth como Bluetooth Low Energy.

7.2.1. API de Bluetooth

Dentro de las funcionalidades que posee, la API permite que las aplicaciones:

- Busquen otros dispositivos Bluetooth.
- Consulte el adaptador Bluetooth local para los dispositivos emparejados.
- Establecer canales RFCOMM.
- Conectarse a sockets especificados por otros dispositivos.
- Transferencia de datos hacia y desde otros dispositivos.

Para que la aplicación utilice esta API se le debe declarar el permiso *BLUETOOTH* y *BLUETOOTH_ADMIN*.

7.2.2. Permisos del sistema

Android es un sistema operativo con privilegios independientes, en el que cada aplicación se ejecuta con una identidad distinta, aislando las aplicaciones entre sí y del sistema operativo.

La seguridad de Android consiste en que ninguna aplicación, de manera predeterminada, posee acceso a los datos privados de los usuarios, leer archivos de otra aplicación o escribir en ellos, acceder a una red, mantener el dispositivo activo, entre otros. Por lo que en las aplicaciones se deben declarar los permisos necesarios estáticamente y luego, el sistema operativo solicita al usuario su consentimiento al instalar la aplicación o al utilizarla.

Para usar funciones protegidas del dispositivo, se debe incluir las etiquetas <*uses-permission*> en el manifiesto de la aplicación.

7.2.3. Manifiesto de la aplicación

Todas las aplicaciones poseen un manifiesto, el cual es llamado AndroidManifiest.xml ubicado en el directorio raíz.

El archivo manifiesto es el encargado de proporcionar información esencial sobre la aplicación a sistema Android. Esta información es requerida por el sistema para poder ejecutar la aplicación.

El manifiesto tiene por objetivo:

- Nombrar al paquete Java para la aplicación, el cual es un identificador único.
- Describir los componentes de la aplicación como actividades y servicios.
- Declara el mínimo nivel de Android API que requiere la aplicación.

La siguiente tabla muestra algunos elementos utilizados por la aplicación, escritos en su manifiesto.

Elemento	Descripción
<activity>	Declara una actividad que implementa parte de la interfaz del usuario visual de la aplicación.
<application>	Dentro de esta etiqueta se declaran todos los elementos que posee y sus atributos.
<category>	Agrega un nombre a un inter-filter.
<intent-filter>	Especifica los objetos de acción a los que puede responder una actividad o servicio. Declara lo que la actividad o servicio puede hacer.
<manifiest>	Es el elemento raíz, debe contener un elemento <application> y especificar los atributos de los paquetes.
<meta-data>	Entrega un nombre y un valor para el ítem.
<uses-permission>	Solicita los permisos que se deben otorgar a la aplicación para su correcto funcionamiento. Es el usuario quien otorga los permisos durante la instalación de la aplicación o durante la ejecución.

Tabla 7-9: Elementos utilizados en manifiesto de la aplicación móvil.

Los permisos del usuario declarados en el manifiesto de la aplicación deben ser *BLUETOOTH* y *BLUETOOTH_ADMIN*.

Permiso	Descripción
BLUETOOTH	Permite que las aplicaciones se conecten a dispositivos Bluetooth vinculados.
BLUETOOTH_ADMIN	Permite que las aplicaciones escaneen y se emparejen a dispositivos Bluetooth.

Tabla 7-10: Permisos de usuario Manifiesto.

7.2.4. Clases API

Las clases públicas principales utilizadas por la aplicación.

Clase	Descripción
BluetoothAdapater	Representa el adaptador Bluetooth del dispositivo local.
BluetoothDevice	Representa un dispositvo Bluetooth remoto.
BluetoothSocket	Conector Bluetooth

Tabla 7-11: Clases públicas aplicación móvil.

La clase BluetoothAdapter representa el adaptador Bluetooth del dispositivo local. Permite realizar tareas fundamentales del Bluetooth, como iniciar descubrimiento de dispositivos, consultar los dispositivos emparejados e instanciar un dispositivo.

La clase bluetoothDevice representa un dispositivo. Permite crear una conexión con el dispositivo respectivo o realizar consultas sobre el mismo, como nombre, dirección, clase y estado del enlace.

La clase BluetoothSocket crea un conector, funciona de manera similar a los sockets TCP. Cuando la conexión es aceptada, devuelve un socket para administrar la conexión. El tipo utilizado de socket Bluetooth es RFCOMM, que es compatible con las API de Android, orientado al transporte de *streaming* a través de Bluetooth.

7.2.5. Clases creadas

Se explicarán a grandes rasgos cómo funcionan las clases principales de la aplicación.

Clase	Descripción
ListaDispositivos	Es la encargada de listar todos los dispositivos vinculados y/o disponibles para vincular. Los dispositivos son mostrados con la MAC correspondiente.
PrincipalActivity	Es la encargada de generar y administrar las conexiones y transferencia de datos, entre el dispositivo y el servidor alojado en la Raspberry.
workerThread	Permite la creación de hilos de ejecución.

Tabla 7-12: Descripción clases aplicación móvil.

7.2.6. Funciones

Las principales funciones se describirán en la siguiente tabla.

Función	Descripción
getDefaultAdapter	Obtiene el identificador al adaptador Bluetooth predeterminado.
sendMsg	Envía un mensaje mediante Bluetooth al dispositivo receptor.
getInputStream	Obtiene el flujo de entrada del subproceso.
PairedDevices	Obtiene los dispositivos que actualmente se encuentran emparejados.

Tabla 7-13: Descripción funciones principales aplicación móvil.

7.2.7. Variables

Algunas variables utilizadas son:

Variable	Tipo – Descripción
SOLICITA_ACTIVACION	STATIC FINAL – contiene el estado de activación Bluetooth.
SOLICITA_CONEXIÓN	STATIC FINAL – contiene el estado de conexión entre dispositivos.
mUUID	UUID – Contiene en forma de string el valor de UUID del servidor.
mBluetoothAdapter	BLuetoothAdapter – Adaptador Bluetooth
mBluetoothDevice	BluetoothDevice – conexión Buetooth.
mBluetoothSocket	BluetoothSocket – socket Bluetooth
delimitador	FINAL BYTE – Posee el carácter delimitador del mensaje.
ReadBufferPosition	INT – Contador de la posición para lectura del buffer.
abreLista	INTENT - Variable que guarda la nueva actividad.
nombreBluetooth	String – Contiene el nombre del dispositivo actual.
macBluetooth	String – Contiene el MAC del dispositivo actual.

Tabla 7-14: Principales variables utilizadas en aplicación móvil.

8. Capítulo: Aplicación y pruebas

En este capítulo se expondrán las capturas de pantalla de la aplicación funcionando y las pruebas realizadas para comprobar su correcto funcionamiento.

8.1. Aplicación

Las siguientes imágenes son capturas de la aplicación ejecutándose en un celular LG G4 Stylus LTE.

En la primera imagen se puede encontrar el icono de la aplicación.

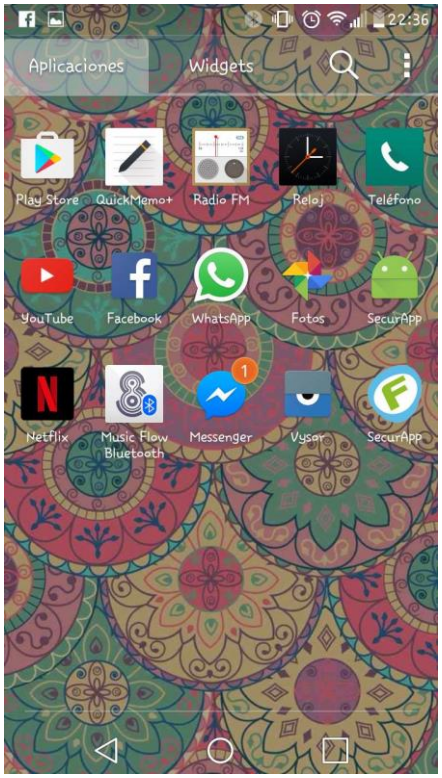


Ilustración 8.1: Imagen icono aplicación.

Al abrir la aplicación ésta automáticamente verificará si el Bluetooth del dispositivo se encuentra encendido. En caso contrario, solicitará al usuario habilitar la opción del Bluetooth, lo cual se puede apreciar en las siguientes imágenes.

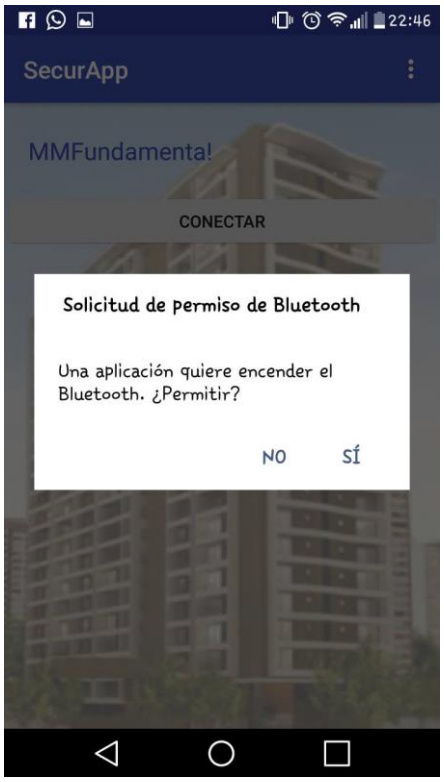


Ilustración 8.2: Solicitud Bluetooth aplicación.

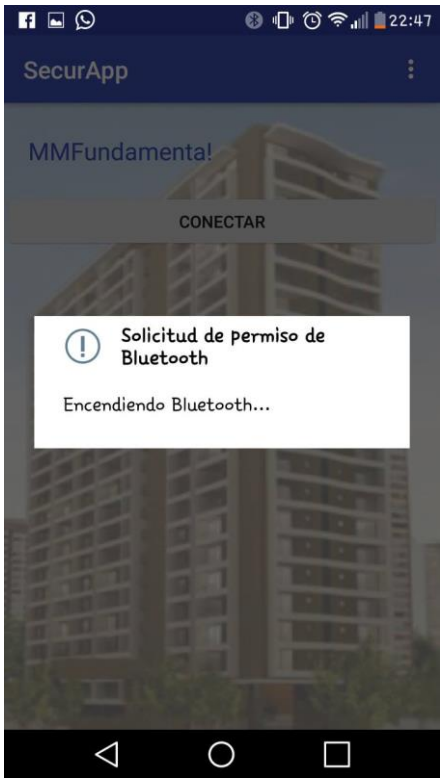


Ilustración 8.3: Encendiendo Bluetooth aplicación.

Ilustración 8.4: Bluetooth activado.

Una vez encendido el Bluetooth, el botón “CONECTAR” se encuentra habilitado. Al presionar el botón, se despliega la lista con todos los dispositivos Bluetooth que se encuentran emparejados al celular o Tablet. Se debe seleccionar “mm-Fundamenta” para que se genere un canal y el servidor esté listo para escuchar.

Ilustración 8.5: Vista principal aplicación.

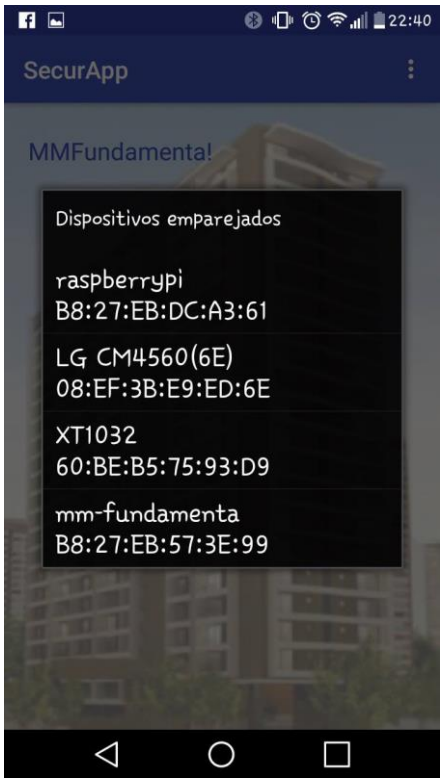


Ilustración 8.6: Lista dispositivos emparejados.

Cuando el dispositivo se encuentra conectado a la red Bluetooth “mm-Fundamenta” se despliegan las opciones habilitadas para el usuario de acuerdo con el nivel de

accesibilidad que posee dentro del sistema, mostrando sólo los botones a los que tiene acceso.

La siguiente imagen muestra la pantalla de un usuario nivel 3.

Ilustración 8.7: Opciones aplicación.

La siguiente tabla describe la funcionalidad de cada botón.

Botón	Funcionalidad
Puerta	Solicitar acceso abriendo la puerta principal peatonal del inmueble.
Portón	Solicitar acceso por el portón vehicular.
Primer piso	Solicitar que el ascensor se dirija al primer piso.
Mi piso	Solicitar que el ascensor se dirija al piso al que se encuentra asociado el individuo.

Tabla 8-1: Funcionalidad opciones aplicación.

8.2. Pruebas

Se realizaron pruebas de comunicación y de permisos.

8.2.1. Pruebas de comunicación

Para realizar la prueba de comunicación y lectura de los datos enviados por la aplicación se visualiza el programa creado en Python, el cual actúa de servidor Bluetooth bajo el protocolo RFCOMM, creando un canal de radio frecuencia que se encuentra permanente escuchando (Ilustración primera), al llegar peticiones (Ilustraciones 19, 20, 21 y 22) desde la aplicación del usuario, el servidor genera salidas y retorna un mensaje emergente a la aplicación del estado de la solicitud "denegado" o "permitido" el cual puede ser leído por el usuario desde su dispositivo.

```
pi@raspberrypi:~/Desktop $ sudo python rfcomm-server.py
rfcomm-server.py:13: RuntimeWarning: This channel is already in use, continuing
anyway.  Use GPIO.setwarnings(False) to disable warnings.
  GPIO.setup(23, GPIO.OUT)
Esperando conexion en RFCOMM canal 1
```

Ilustración 8.8.8: Servidor Bluetooth en ejecución.

```
Esperando conexion en RFCOMM canal 1
Se acepta conexiòn desde  ('00:34:DA:BE:86:9A', 1)
received [ascensor]
sending [Porton abierto!]
```

Ilustración 8.9: Petición de ascensor.

```
Esperando conexion en RFCOMM canal 1
Se acepta conexiòn desde  ('00:34:DA:BE:86:9A', 1)
received [accesoPorton]
sending [Porton abierto!]
```

Ilustración 8.10: Petición de portón.

```
Esperando conexion en RFCOMM canal 1
Se acepta conexiòn desde  ('00:34:DA:BE:86:9A', 1)
received [accesoPuerta]
sending [Puerta abierta!]
```

Ilustración 8.11: Petición de puerta principal.

8.2.2. Usuarios no registrados

Cuando un usuario no se encuentra registrado en la base de datos, posee la aplicación en su dispositivo y alguna vez se emparejó al sistema, la aplicación se conecta a la red Bluetooth y se le despliegan todas las opciones, pero al realizar alguna petición, esta no será procesada y se le indica al usuario por medio de la interfaz de la aplicación que no se encuentra registrado.

Ilustración 8.12 Aplicación usuario no registrado.

La respuesta anterior es generada por el servidor, el que realiza la consulta a la base de datos y emite el mensaje a mostrar al usuario.

```
Esperando conexion en RFCOMM canal 1
Se acepta conexiòn desde  ('00:34:DA:BE:86:9A', 1)
0
Usuario no válido
Enviando[No cuenta con permiso para ingresar!]
Esperando conexion en RFCOMM canal 1
```

Ilustración 8.13: Servidor usuario no registrado.

8.2.3. Usuarios registrados y con permisos

Para esta prueba, un usuario debe ingresar al sistema, la aplicación debe estar instalada y el dispositivo emparejado. Cuando el usuario realiza alguna petición. Esta se envía al sistema, se procesa y emite la salida. En la pantalla del usuario se puede apreciar el estado de su solicitud.

Ilustración 8.14 Aplicación usuario registrado y con permiso.

Para este caso el servidor reacciona de dos formas, emitiendo un mensaje, el cual se muestra en la aplicación y produciendo la orden para emitir la acción como abrir puerta, abrir portón vehicular o solicitar ascensor.

```
Esperando conexion en RFCOMM canal 1
Se acepta conexiòn desde  ('00:34:DA:BE:86:9A', 1)
1
received [puerta]
Enviando[Puerta abierta !]
Esperando conexion en RFCOMM canal 1
```

Ilustración 8.15 Servidor usuario registrado y con permiso.

8.2.4. Usuarios registrados sin permiso

Para realizar esta prueba se ingresa al usuario a la base de datos con nivel de autorización “0” y se le instala la aplicación.

Cuando el usuario realiza alguna petición el sistema responde con el mensaje “Usted no posee autorización”, el cual puede ser leído en la pantalla de la aplicación.

Ilustración 8.16: Aplicación usuario registrado y sin permiso.

El servidor reconoce al usuario, obtiene su nivel de acceso y emite la respuesta.

```
Esperando conexion en RFCOMM canal 1
Se acepta conexiòn desde  ('00:34:DA:BE:86:9A', 1)
1
0
Usuario inhabilitado
Usuario no válido
Enviando[No cuenta con permiso para ingresar!]
Esperando conexion en RFCOMM canal 1
```

Ilustración 8.17 Servidor usuario registrado y sin permiso.

8.3. Verificación y validación

Elemento	Verificación
Código aplicación	El código compila sin errores ni *warnings*.
Dispositivos diversos	La aplicación funciona correctamente en distintos celulares, probados LG y Motorola. La aplicación funciona simultáneamente para más de un dispositivo.
Solicitud Bluetooth	La aplicación solicita el acceso de Bluetooth y en caso de confirmación lo activa automáticamente si éste se encuentra desactivado.
Vistas aplicación	La aplicación cuenta con dos vistas que funcionan correctamente.
Estado	La aplicación mantiene al usuario informado sobre el estado de su petición a través de mensajes emergentes y una pequeña ventana de diálogo.
Servidor RFCOM	El servidor RFCOMM se encuentra escuchando permanentemente en busca de peticiones.

Tabla 8-2: Verificación.

Elemento	Validación
Instalación	El Smartphone permite la instalación de aplicaciones de terceros, y en este caso la aplicación de seguridad creada. Se realiza mediante el traspaso del archivo ".apk" hacia el Smartphone.
Emparejamiento	El dispositivo debe tener una versión 3.0 o superior de Bluetooth y debe permitir el emparejamiento hacia otros dispositivos.
Comunicación	Los comandos enviados a través de los botones desplegados en la aplicación deben permitir el control de los GPIO de la Raspberry, pudiendo así controlar los dispositivos comandados por el servidor como los accesos al edificio, portón o ascensor.

Tabla 8-3: Validación.

9. Capítulo: Conclusiones y resultados

En este capítulo se discutirán los resultados obtenidos, analizando el cumplimiento de los requisitos iniciales, se mencionarán los posibles pasos a seguir y las aplicaciones que se le podrían agregar para complementar este sistema.

Además, se comentarán los aportes realizados.

9.1. Resultados

Recapitulando, el sistema desarrollado consta de una Raspberry Pi 3 modelo B llamado nodo, el cual genera una red Bluetooth permitiendo la comunicación entre éste y distintos dispositivos móviles. Además, emite señales a través de los pines de comunicaciones llamados GPIO los cuales deberán ser conectados a los ascensores, puertas y portones que posea el inmueble.

El nodo posee una base de datos local que maneja un registro de todos los usuarios con datos como nombre, rut, departamento, teléfono, permisos y MAC del dispositivo asociado. La MAC del dispositivo funciona como un identificador único del emisor para el sistema receptor, nodo, representando al usuario y en base a ella se realizan las consultas de permisos al emitir peticiones.

Las peticiones son emitidas por el dispositivo móvil del usuario y cuenta con las opciones de solicitar ascensor y desbloqueo de puertas de acceso tanto peatonales como vehiculares. Éstas son enviadas por el canal RFCOMM que genera el nodo cuando se establece la conexión Bluetooth entre el dispositivo y el sistema.

Los permisos del usuario poseen un rol fundamental en el sistema, ya que éstos poseen la información de seguridad a la cual puede optar el usuario y es en base a la interpretación del sistema de esta información si es que permite o deniega el acceso.

El sistema de seguridad desarrollado luego de interpretar la información emitida por el usuario, o más bien por su dispositivo móvil, genera dos respuestas. Una es a través de la aplicación móvil, generando un mensaje visible para el usuario mostrándole a éste el estado de su petición, es decir, si la petición se realzará o se negará. La otra respuesta emitida por el sistema se desarrolla a través de los pines GPIO del nodo, por los cuales se emite un voltaje alto de salida para confirmar la petición o no se genera para denegar la petición.

Como se ha mencionado anteriormente, las peticiones son enviadas desde el dispositivo móvil del usuario, esto se hace a través de una aplicación ejecutada en el smartphone.

La aplicación móvil genera la conexión Bluetooth entre el dispositivo y el nodo, despliega los botones disponibles, los cuales pueden ser abrir puerta, portón o solicitar ascensor. Al pulsar algunos de estos botones se envía el requerimiento como un mensaje a través del canal Bluetooth y la respuesta de éste se puede apreciar en la pantalla del aparato móvil, aplicación.

Cabe mencionar que para que todo lo anteriormente mencionado funcione correctamente se debe emparejar al sistema el dispositivo móvil.

9.2. Conclusiones

Al finalizar el desarrollo de este proyecto y revisar los puntos más importantes de este, es posible mencionar lo siguiente:

- El sistema cuenta como tecnología principal de comunicación con Bluetooth, entre los distintos dispositivos móviles y el servidor, posee un sistema de registro de todos los usuarios, el cual es utilizado para permitir o denegar el acceso. Además, el sistema alerta cuando un individuo no autorizado solicita ingresar.
- El sistema desarrollado cuenta con un registro histórico de todas las peticiones que se les han hecho vinculadas a la MAC de dispositivo.
- La aplicación puede ser instalada en dispositivos que cuenten con sistema operativo Android 4.0.3 o superior y es ella la encargada de realizar las peticiones al sistema.

Debido a lo anterior, se puede decir que el sistema cumple con los dos objetivos principales solicitado por el cliente, el cual es el uso del Bluetooth y smartphones. Gracias a la utilización de éstos, el sistema no necesita retener a los usuarios una gran cantidad de tiempo, por lo que resulta ser, no invasivo.

El sistema de seguridad desarrollado aprovecha la relación de los usuarios con la tecnología, agregando a ésta un servicio útil y confiable.

Para concluir, se puede decir, que el sistema creado es bastante seguro ya que cuenta con dos permisos para funcionar, los cuales son dados al momento de ingresar al usuario al sistema, a través de la vinculación del dispositivo al servidor y de las autorizaciones que son otorgadas gracias a la base de datos.

9.3. Trabajo futuro

La tecnología cada día avanza a pasos agigantados y con esto un nuevo concepto que ha llegado para quedarse: la “internet de las cosas”. El internet de las cosas se refiere a darle conexión a todo tipo de dispositivos, especialmente los de usos diarios, a los cotidianos, como los electrodomésticos de los hogares, automóviles, relojes, entre otros.

Internet de las cosas se posiciona como una tecnología que permitirá mejorar y simplificar la vida, pudiendo satisfacer necesidades básicas como operar una estufa, aire acondicionado o un sistema de seguridad completo.

Para la realización del internet de las cosas es necesario contar con dispositivos conectados a la red.

De acuerdo con lo anterior y considerando el sistema desarrollado que ya cuenta con diversos dispositivos conectados a una red, se podría pensar en complementarlo con otros como sensores de temperatura que automáticamente enciendan o apaguen equipos de aires acondicionado o estufas, sensores de oscuridad que activen luz, sensores de detección de estado de puertas que generen alarmas.

Por otro lado, se puede integrar un sistema automatizado de cobro de gastos comunes, que cumpla un rol administrativo, que genere correo masivo para citaciones a reuniones dentro del condominio, que genere alertas a los usuarios en caso de siniestros, entre muchas cosas más.

Además, si bien el sistema desarrollado está pensado para la utilización en proyectos habitacionales, también puede utilizarse en otros tipos de rubros, como universidades, bibliotecas, colegios, empresas públicas y privadas, eventos masivos, entro otros.

Así es como las posibilidades de expansión son infinitas y algunas de muy bajo costo, todas con el fin de simplificar y ayudar a los usuarios, considerando que son ellos quienes también buscan la tecnología y facilidad en su día a día.

Referencias

[1] Paz Ciudadana y Cfk Adimark, «Delincuencia y opinión Pública,» 2017.

[2] Inmobiliaria Fundamenta, «Percepción de satisfacción,» Santiago, 2015.

[3] SecuritySystem, «cms.dsc.com,» 2005. [En línea]. Available: http://cms.dsc.com/download2.php?t=1&id=12861. [Último acceso: 10 Mayo 2017].

[4] s. Bhattacharya, «https://www.newscientist.com,» 30 Marzo 2005. [En línea]. Available: https://www.newscientist.com/article/dn7209-electronic-tags-for-eggs-sperm-and-embryos/. [Último acceso: 31 Mayo 2017].

[5] hitachi, «www.hitachi.com,» 6 Febrero 2006. [En línea]. Available: http://www.hitachi.com/New/cnews/060206.html. [Último acceso: 31 Mayo 2017].

[6] BBC, «news.bbc.co.uk,» 23 Febrero 2007. [En línea]. Available: http://news.bbc.co.uk/2/hi/technology/6389581.stm. [Último acceso: 02 Junio 2017].

[7] S. Fuentes, «La seguridad del RFID,» Santiago, 2009.

[8] TSF, «https://sistemas-rfid.es,» [En línea]. Available: https://sistemas-rfid.es/index.php?r=rfid-fabrica.html. [Último acceso: 2 Junio 2017].

[9] D. Goodin, «www.theregister.co.uk,» 2 Febrero 2009. [En línea]. Available: http://www.theregister.co.uk/2009/02/02/low_cost_rfid_cloner/. [Último acceso: 30 Mayo 2017].

[10] A. Asuán, «mcompro,» 10 Febrero 2015. [En línea]. Available: https://www.muycomputerpro.com/2015/02/10/seguridad-en-la-tecnologia-nfc. [Último acceso: 5 Junio 2017].

[11] International Organization for Standardization, «www.iso.org,» ISO/IEC 18092:2004, Abril 2004. [En línea]. Available: https://www.iso.org/standard/38578.html. [Último acceso: 15 Junio 2017].

[12] nfc, «NFC,» [En línea]. Available: https://nfc-forum.org/our-work/specifications-and-application-documents/specifications/nfc-forum-technical-specifications/. [Último acceso: 15 Junio 2017].

[13] G. M. Mozos, «redseguridad,» [En línea]. Available: http://www.redseguridad.com/opinion/articulos/riesgos-y-soluciones-para-la-tecnologia-nfc.

[14] D. M. D. M. R.Cappelli, «Combining Fingerprint Classifiers,» de *Workshop on Multiple Classifiers System*, 2000, pp. 351 - 361.

[15] L. Padilla, «www.gae.ucm.es,» [En línea]. Available: http://www.gae.ucm.es/~padilla/extrawork/tracks.html. [Último acceso: 18 Junio 2017].

[16] BIT, «www.tec-mex.com,» [En línea]. Available: https://www.tec-mex.com.mx/promos/bit/bit0703-msr.htm. [Último acceso: 20 Julio 2017].

[17] A. J. S. Li, Handbook Of Face Recognition, Springer, 2004.

[18] A. K. Gary Bradski, Learning OpenCV, O'Reilly, 2008.

[19] l. H. j. L. V. M. V. c. Havran, «Independent Component Analysis for Face Authentication, Proceedings-Knowledge-based Intelligent Information and Engineering System,» Crema, italia, 2002.

[20] siconmobile, «Google Play,» 17 Diciembre 2015. [En línea]. Available: https://play.google.com/store/apps/details?id=com.grupoarpada.siconmobile&hl=es. [Último acceso: 15 Julio 2017].

[21] Safecard, «http://safecardapp.com/,» [En línea]. Available: http://safecardapp.com/. [Último acceso: 21 Julio 2017].

[22] S. A. Technologies, «Google Play,» [En línea]. Available: https://play.google.com/store/apps/details?id=com.safecard.android&hl=es_419. [Último acceso: 10 Septiembre 2017].

[23] J. Daugam, «How iris recognition work,» de *Transactions on circuits and System for Video Technology*, 2004, pp. 21-30.

[24] J. Daugman, «Theimportance of being random: statiscal principles of iris recognition,» de *Pattern Recognition* , 2003, pp. 28-290.

[25] Android, «Android,» [En línea]. Available: https://www.android.com/. [Último acceso: 29 Julio 2017].

[26] Android, «Android,» [En línea]. Available: https://www.android.com/intl/es-419_mx/history/#/marshmallow. [Último acceso: 15 Agosto 2017].

[27] M. S. Zavia, «Gizmodo,» 10 Mayo 2015. [En línea]. Available: http://es.gizmodo.com/7-anos-de-historia-la-evolucion-de-la-homescreen-de-an-1734716500. [Último acceso: 13 Agosto 2017].

[28] Android, «developer.android.com,» [En línea]. Available: https://developer.android.com/guide/platform/index.html?hl=es-419. [Último acceso: 3 Septiembre 2017].

[29] Bluetooth, «www.bluetooth.com,» [En línea]. Available: https://www.bluetooth.com/. [Último acceso: 10 Septiembre 2017].

[30] Android, «developer.android.com,» [En línea]. Available: https://developer.android.com/guide/topics/connectivity/bluetooth.html?hl=es-419. [Último acceso: 16 Septiembre 2017].

[31] Memorias Multidisciplinarias, «Fortalecimiento del Desarrollo de Competencias Transversales en la Formación del Profesional USM - Foco Q1 Q2,» [En línea]. Available: http://competenciastransversales.usm.cl. [Último acceso: 20 Octubre 2017].

A. Anexo

B. Manifiesto Aplicación

```
<uses-permission android:name="android.permission.BLUETOOTH" />
<uses-permission android:name="android.permission.BLUETOOTH_ADMIN" />
```